Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Copyright© 2022 Trinity Guard LLC. All rights reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. What’s New</td>
<td>5</td>
</tr>
<tr>
<td>2. TGDetect Introduction</td>
<td>6</td>
</tr>
<tr>
<td>2.1 Features</td>
<td>7</td>
</tr>
<tr>
<td>3. Getting Started</td>
<td>9</td>
</tr>
<tr>
<td>3.1 Log Into TGDetect</td>
<td>11</td>
</tr>
<tr>
<td>3.2 Working with TGDetect</td>
<td>12</td>
</tr>
<tr>
<td>4. Defaults</td>
<td>13</td>
</tr>
<tr>
<td>4.1 Working with TGDetect Defaults</td>
<td>14</td>
</tr>
<tr>
<td>4.2 Display TGDetect Defaults</td>
<td>15</td>
</tr>
<tr>
<td>4.3 Manage TGDetect Defaults</td>
<td>16</td>
</tr>
<tr>
<td>4.4 Run TGDetect Default Setting Reports</td>
<td>20</td>
</tr>
<tr>
<td>5. Monitors</td>
<td>22</td>
</tr>
<tr>
<td>5.1 Working with Monitors</td>
<td>23</td>
</tr>
<tr>
<td>5.1.1 Display Monitors</td>
<td>24</td>
</tr>
<tr>
<td>5.1.2 Manage Monitors</td>
<td>26</td>
</tr>
<tr>
<td>5.1.3 Run Monitor Master Reports</td>
<td>29</td>
</tr>
<tr>
<td>5.2 Command Monitor</td>
<td>31</td>
</tr>
<tr>
<td>5.2.1 Working with Command Monitor</td>
<td>32</td>
</tr>
<tr>
<td>5.2.2 Display Command Monitor Rules</td>
<td>33</td>
</tr>
<tr>
<td>5.2.3 Display Command Monitor Rule Criteria</td>
<td>35</td>
</tr>
<tr>
<td>5.2.4 Display Command Monitor Alerts</td>
<td>37</td>
</tr>
<tr>
<td>5.2.5 Display Command Monitor Activity Log</td>
<td>39</td>
</tr>
<tr>
<td>5.2.6 Manage Command Monitor Rules</td>
<td>40</td>
</tr>
<tr>
<td>5.2.7 Manage Command Monitor Rule Criteria</td>
<td>42</td>
</tr>
<tr>
<td>5.2.8 Manage Command Monitor Alerts</td>
<td>44</td>
</tr>
<tr>
<td>5.2.9 Run Command Monitor Reports</td>
<td>47</td>
</tr>
<tr>
<td>5.3 History Log Monitor</td>
<td>51</td>
</tr>
<tr>
<td>5.3.1 Working with History Log Monitor</td>
<td>52</td>
</tr>
<tr>
<td>5.3.2 Display History Log Rules</td>
<td>53</td>
</tr>
<tr>
<td>5.3.3 Display History Log Rule Criteria</td>
<td>55</td>
</tr>
<tr>
<td>5.3.4 Display History Log Alerts</td>
<td>57</td>
</tr>
<tr>
<td>5.3.5 Display History Log Activity Log</td>
<td>59</td>
</tr>
<tr>
<td>5.3.6 Manage History Log Rules</td>
<td>60</td>
</tr>
<tr>
<td>5.3.7 Manage History Log Rule Criteria</td>
<td>62</td>
</tr>
<tr>
<td>5.3.8 Manage History Log Alerts</td>
<td>67</td>
</tr>
<tr>
<td>5.3.9 Run History Log Reports</td>
<td>70</td>
</tr>
<tr>
<td>5.4 Journal Monitor</td>
<td>71</td>
</tr>
<tr>
<td>5.4.1 Working with Journal Monitor</td>
<td>72</td>
</tr>
<tr>
<td>5.4.2 Display Journal Monitor Rules</td>
<td>73</td>
</tr>
<tr>
<td>5.4.3 Display Journal Monitor Rule Criteria</td>
<td>76</td>
</tr>
<tr>
<td>5.4.4 Display Journal Monitor Alerts</td>
<td>77</td>
</tr>
<tr>
<td>5.4.5 Display Journal Monitor Activity Log</td>
<td>78</td>
</tr>
<tr>
<td>5.4.6 Manage Journal Monitor Rules</td>
<td>79</td>
</tr>
<tr>
<td>5.4.7 Manage Journal Monitor Rule Criteria</td>
<td>81</td>
</tr>
<tr>
<td>5.4.8 Manage Journal Monitor Alerts</td>
<td>83</td>
</tr>
<tr>
<td>5.4.9 Run Journal Monitor Reports</td>
<td>85</td>
</tr>
<tr>
<td>5.5 Message Queue Monitor</td>
<td>88</td>
</tr>
<tr>
<td>5.5.1 Working with the Message Queue Monitor</td>
<td>89</td>
</tr>
<tr>
<td>5.5.2 Display Message Queue Rules</td>
<td>90</td>
</tr>
<tr>
<td>5.5.3 Display Message Queue Rule Criteria</td>
<td>92</td>
</tr>
<tr>
<td>5.5.4 Display Message Queue Alerts</td>
<td>94</td>
</tr>
<tr>
<td>5.5.5 Display Message Queue Activity Log</td>
<td>95</td>
</tr>
<tr>
<td>5.5.6 Manage Message Queue Rules</td>
<td>96</td>
</tr>
<tr>
<td>5.5.7 Manage Message Queue Rule Criteria</td>
<td>98</td>
</tr>
<tr>
<td>5.5.8 Manage Message Queue Alerts</td>
<td>103</td>
</tr>
<tr>
<td>5.5.9 Run Message Queue Reports</td>
<td>106</td>
</tr>
<tr>
<td>5.6 SIEM Monitor</td>
<td>110</td>
</tr>
<tr>
<td>5.6.1 Working with SIEM Monitor</td>
<td>111</td>
</tr>
<tr>
<td>5.6.2 Display SIEM Monitor Rules</td>
<td>112</td>
</tr>
<tr>
<td>5.6.3 Display SIEM Monitor Rule Criteria</td>
<td>114</td>
</tr>
</tbody>
</table>
5.6.4 Manage SIEM Monitor Rules ................................................. 116
5.6.5 Manage SIEM Monitor Rule Criteria ..................................... 118
5.6.6 Run SIEM Reports ............................................................... 120
6. Rules ...................................................................................... 123
   6.1 Working with Monitor Rules .................................................. 124
7. Activity Log ............................................................................. 126
   7.1 Working with Monitor Activity Log ......................................... 127
8. Reports ..................................................................................... 128
   8.1 Working with Monitor Reports ............................................... 129
9. Groups ..................................................................................... 130
   9.1 User Groups .......................................................................... 131
      9.1.1 Working with User Groups ............................................... 132
      9.1.2 Display List of User Groups ............................................. 133
      9.1.3 Display List of Users in a Group ...................................... 136
      9.1.4 Manage User Groups ..................................................... 138
      9.1.5 Manage Users in a Group .............................................. 141
   9.2 Network/Server Groups ......................................................... 144
      9.2.1 Working with Network/Server Groups .............................. 145
10. Email/Syslog Setup ................................................................. 146
   10.1 Working with Email/Syslog Setup ............................................ 147
      10.1.1 Email Setup .................................................................. 148
      10.1.1.1 Working with Email Alerts ........................................ 149
      10.1.1.2 Working with Email Setup ........................................ 150
      10.1.1.2.1 Manage Email Setup ............................................ 151
      10.1.2 Syslog Setup ................................................................ 157
      10.1.2.1 Working with Syslog Setup ....................................... 158
      10.1.2.1.1 Manage Syslog Setup .......................................... 159
11. Appendices ............................................................................. 162
   11.1 APPENDIX - TGdetect Revisions ......................................... 163
      11.1.1 Version 2.4 - TGdetect User Guide Revisions .................. 164
      11.1.2 Version 2.3 - TGdetect User Guide Revisions ................. 165
      11.1.3 Version 2.2 - TGDefect User Guide Revisions ............... 166
   11.2 APPENDIX - TGdetect Collectors ......................................... 168
   11.3 APPENDIX - TGdetect Built-in History Log (QHST) Rules .......... 178
   11.4 APPENDIX - TG Fix ............................................................. 181
   11.5 APPENDIX - TG Management .............................................. 182
   11.6 APPENDIX - TG Save and Restore ........................................ 183
What's New

<table>
<thead>
<tr>
<th>Version 2.4 - TGDetect User Guide Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhancements</td>
</tr>
<tr>
<td>• Addition of SEIM batch configuration details</td>
</tr>
<tr>
<td>• SIEM Batch Process enhanced support Message Queues (*MSGQ) and History Log (*QHST)</td>
</tr>
</tbody>
</table>

See also

APPENDIX - TGDetect Revisions
TGDetect Introduction

**TGDetect** allows you to monitor iSeries systems for security and system events. This is done by monitoring system logs, message queues, and system journals. When a critical system event is detected, TGDetect sends an alert (i.e., email, system messages, etc.) to the security administrator or forwards the information to an SIEM (Security Information and Event Management) system so that appropriate actions might be taken.

**Note:** While you can use TGSDetect as a standalone product, it is also one component of a powerful security suite. For more information about the suite or other products in the suite, go to [TrinityGuard.com](http://TrinityGuard.com).

See also

- What's New
- Getting Started
Features

To help you design, manage, and maintain security alerts, TGDetect includes the following product features:

Monitors

Monitors allow you to define (via rules) a policy for overseeing and alerting designated recipients (or third-party tools) when questionable system activities occur.

See Working with Monitors for additional information.

Rules

Rules allow you to define the criteria by which to monitor system activities. When a system action meets the rule criteria defined, TGDetect sends an alert.

See Working with Monitor Rules for additional information.

Alerts

Alerts allow you to send notifications to designated recipients regarding questionable system activities.

See Working with Monitor Alerts for additional information.
Activity Logs
Activity logs allow you to display the complete list of alerts specific to a monitor.
See Working with Monitor Activity Logs for additional information.

Reports
Reports allow you to analyze and share activity log data.
See Working with Monitor Reports for additional information.

Groups
User groups allow you to create rules more efficiently.
See Working with User Groups for additional information.

See also
Features
Getting Started

This topic discusses the following:

- **Actions**
- **Process Flow**
- **Implementation Tasks**

**Actions**

The following TGDetect features allow you to do the following:

- **Monitors** - Enable tracking of system actions
- **Monitor Rules** - Identify which system actions to track
- **Alerts** - Identify recipient and method of notifications when rule criteria are met
- **Activity Log** - Display list of activity alerts
- **Reports** - Generate reports based on activity log entries
- **Groups** - Create a user group to manage rules more efficiently

**Process Flow**

![Process Flow Diagram]

**Implementation Tasks**

There is no single linear process for implementing TGSecure, but the following describes how a typical implementation might work. It's important to remember that security management is an iterative process.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1 | **Set up TGDetect defaults**  
In preparation for monitoring, you must define some basic system defaults (e.g., collections intervals)  
See [Working with TGDetect Defaults](#) for additional information.  
**Tip:** You can also create user groups at this time to make rule maintenance more efficient. |
| 2 | **Start the TGDetect Subsystem**  
To enable monitoring, you must start the TGDetect subsystem.  
**Tip:** You can also stop the TGDetect subsystem at any point to disable all monitors.  
See [Working with Monitors](#) for additional information. |
| 3 | **Enable Monitors**  
Once you start monitoring (via the TGDetect subsystem), you can then enable individual monitors to begin tracking system activities.  
See [Working with Monitors](#) for additional information. |
<table>
<thead>
<tr>
<th></th>
<th>Create Monitor Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>To define the actions you want to monitor, you must create monitor rules with specific criteria. When a system action meets the criteria established, an alert (notifications) is triggered. See <a href="#">Working with Monitor Rules</a> for additional information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Create Alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>To define the designated recipient for a notification, you must create alerts. See <a href="#">Working with Monitor Alerts</a> for additional information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Display Activity Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>To view the alerts generated for a specific monitor, access the activity log for that monitor. See <a href="#">Working with Monitor Activity Logs</a> for additional information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Run Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Run reports to monitor activity and track changes. See <a href="#">Working with Monitor Reports</a> for additional information.</td>
</tr>
</tbody>
</table>

**See also**

- [Log Into TGDetect](#)
- [Features](#)
Log Into TGDetect

Use this task to log into TGDetect.

To log into TGDetect

1) Sign into your IBM i server.

2) At the Selection or command prompt, enter TGMENU.

3) Press Enter. The TG - Main Menu interface is displayed.

4) At the Selection or command prompt, enter 3 (TGDetect). The TGDetect Main menu is displayed.

See also

Getting Started

Working with TGDetect
Working with TGDetect

Follow these steps:

**Step 1:** Setup defaults
- Working with TGDetect Defaults

**Step 2:** Setup monitors
- Working with Monitors

**Step 3:** Setup rules
- Working with Monitor Rules

See also

Getting Started
Defaults

The sections include the following topics:

- Working with TGDetect Defaults
- Display TGDetect Defaults
- Manage TGDetect Defaults
- Run TGDetect Default Setting Reports

See also

Getting Started
Working with TGDetect Defaults

This section describes working with TGDetect system defaults. The default settings are the settings that impact all monitors (i.e., defining data collection intervals, enabling/disabling auditing, starting/stopping subsystems, etc.).

**Tips:** Set your defaults before you begin working with monitors.

This section includes the following topics:

- Display TGDetect Defaults
- Manage TGDetect Defaults
- Run TGDetect Default Setting Reports

See also

TGDetect Introduction
Display TGDetect Defaults

Use this task to display TGDetect defaults. The default settings are the settings that impact all monitors (i.e., defining data collection intervals, enabling/disabling auditing, starting/stopping subsystems, etc.).

Tips: Set your defaults before you begin working with monitors.

Note: In order to work with defaults, you must access the TGDetect Default Setting interface.

To access the Work with TGDetect Default Setting interface

1) Log into TGDetect. The Main menu appears.

2) At the Selection or command prompt, enter 11 (TGDetect Defaults).

3) Press Enter. The Work with TGDetect Default Setting interface is displayed.

See also

Working with TGDetect Defaults
Manage TGDetect Defaults

Use this task to do the following:

- Access the TGDetect Default Settings Interface
- Add Collection Interval Defaults
- Add SIEM Defaults
- Add Auditing Defaults
- Configure SIEM Batch
- Start Subsystem
- Stop Subsystem

**Note:** To manage monitors, access from the **TGDetect Default Settings** interface.

**Access the TGDetect Default Settings Interface**

Use this task to access the interface from which you can modify default settings.

**To access the Working with TGDetect Default Settings interface**

1) Access the TGDetect **Main** menu.
2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**. The **TGDetect Default Setting** interface is displayed.

**Add Collection Interval Defaults**

Use this task to add timing for the collection of system activities for specific monitor types.

**To add collection intervals**

1) Access the **TGDetect Default Setting** interface.
2) Complete the following fields under **Collection Intervals**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Log</td>
<td>Enter (in seconds) how often to check the history log monitor for alerts that required sending</td>
</tr>
<tr>
<td>Message Queue</td>
<td>Enter (in seconds) how often to check the message queue monitor for alerts that required sending</td>
</tr>
<tr>
<td>Real-time Journal</td>
<td>Enter (in seconds) how often to check the journal monitor for alerts that required sending</td>
</tr>
</tbody>
</table>

**Tip:** Press **F1** (Help) to access field descriptions.

3) Press **Enter**.
Add SIEM Defaults

Use this task to change the SIEM (Security Information and Event Management) defaults.

To add SIEM defaults

1) Access the TGDetect Default Setting interface.

2) Complete the following fields under SIEM Configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Interval</td>
<td>Enter (in minutes) how often to check the SIEM monitor for alerts that required sending</td>
</tr>
<tr>
<td>Log format</td>
<td>Enter one of the following:</td>
</tr>
<tr>
<td></td>
<td>*GELF - Send data in Graylog extended log format</td>
</tr>
<tr>
<td></td>
<td>*JSON - Send data in JavaScript object notation format</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Send data in syslog format</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the SIEM server</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port to use for SIEM communication</td>
</tr>
<tr>
<td>Protocol</td>
<td>Enter one of the following:</td>
</tr>
<tr>
<td></td>
<td>*TCP - Use transmission control protocol</td>
</tr>
<tr>
<td></td>
<td>*SSL - Secure socket layer protocol</td>
</tr>
<tr>
<td></td>
<td>*UDP - User Datagram protocol</td>
</tr>
</tbody>
</table>

3) Press Enter.

Add Auditing Defaults

Use this task to change the auditing defaults.

Tip: Auditing must be enabled to run change reports. See Working with Monitor Reports for a list of reports available.

To add audit defaults

1) Access the TGDetect Default Setting interface.

2) Complete the following fields under SIEM Configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Journal</td>
<td>Enter the journal in which to store alert data</td>
</tr>
<tr>
<td>Note:</td>
<td>The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.</td>
</tr>
<tr>
<td>Audit Journal Library</td>
<td>Enter the library in which the journal is stored</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------</td>
</tr>
</tbody>
</table>
| Audit Configuration Changes | Enter one of the following: Y - Enable tracking of changes N - Disable tracking of changes  
**Tip:** Set this flag to Y if you plan to run ISL change reports.  
**Note:** There are multiple product modules (e.g., network security, access escalation, inactive session lockdown, etc.) in which you can track configuration changes. Therefore, if you see *NONE* in the comment field, this indicates that configuration changes are not being tracked in any module. This is common at the time the product is initially installed. If you see *PARTIAL*, this indicates that configuration changes are being tracked in at least one module, but not all modules. If you see *ALL*, this indicates that configuration changes are being tracked in all modules.  
| Alerting User Profile | User profile who will be identified as the sender of alerts. In other words, if an email notification is sent, the user profile you enter here will be identified as the sender of the email. |

3) Press **Enter**.

**Configure SIEM Batch**

Use this task to configure SIEM Batch details.

**Tip:** Press **F1** (Help) to access field descriptions.

**To configure SIEM batch details**

1) Access the **TGDetect Default Setting** interface.

2) Press **F18** (Config SIEM Batch) on your keyboard.

3) Press **Enter**.

**Start Subsystem**

Use this task to start the TGDetect subsystem.

**Note:** You must start the subsystem if you want to begin monitoring. Once you start the subsystem, all enabled monitors will begin overseeing system activities.
To add audit defaults

1) Access the **TGDetect Default Setting** interface.

2) Press **F22** (Start subsystem) on your keyboard.

**Stop Subsystem**

Use this task to stop the TGDetect subsystem.

**Tip:** A quick way to stop all monitors (other than disabling each individual monitor) is to stop the subsystem.

**Note:** You must start the subsystem if you want to begin monitoring. Once you start the subsystem, all enabled monitors will begin overseeing system activities.

**Tip:** A quick way to stop all monitors (other than disabling each individual monitor) is to stop the subsystem.

To add audit defaults

1) Access the **TGDetect Default Setting** interface.

2) Press **F23** (Stop subsystem) on your keyboard.

**See also**

Working with Email Setup
Run TG Detect Default Setting Reports

Use this task to generate the following reports:

- Access the TG Detect Reports Interface
- Run Default Settings Report
- Run Default Settings Change Report

Tip: Refer to the TG Detect Report Reference for a complete list of report definitions.

Note: To work with default setting reports, access from the TG Detect Reports interface.

Access the TG Detect Reports Interface

To access the TG Detect Reports interface

1) Access the TG Secure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TG Detect Reports interface is displayed.

Run Default Settings Report

Use this report to display the list of default settings.

To run the Default Settings Report

1) Access the TG Detect Reports interface.
2) At the Selection or command prompt, enter 2 (Configuration Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 1 (Default Settings).
5) Press Enter.
6) Modify the run criteria as necessary.
7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Default Settings Change Report

Use this report to display the list of changes made the default settings.

Tip: Change auditing must be enabled for data to be present in this report.

To run the Defaults Settings Change Report
1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Change Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 1 (Default Settings).

5) Press **Enter**.

6) Modify the run criteria as necessary.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

- **Working with TGDetect Defaults**
- **Working with Reports**
Monitors

This section includes the following topics:

- Working with Monitors
- Command Monitor
- History Log Monitor
- Journal Monitor
- Message Queue Monitor
- SIEM Monitor

See also

Getting Started
Working with Monitors

This section describes working with monitors. Monitors provide you with a means by which to track system activities that require that an individual (i.e., user or user group) or a log management tool (e.g., Sentinel, ELK, etc.) receives appropriate notifications (alerts).

- Display Monitors
- Manage Monitors
- Run Monitor Master Reports

Monitor Types

The following built-in monitors are available when you initially install TGDetect:

- Command Monitor (CMD)
- History Log Monitor (QHST)
- Journal Monitor (JRN)
- Message Queue Monitor (MSQG)
- SIEM Monitor (Journal Archival)

Tip: You can add custom message queue monitors as required to meet your security policy needs.

Monitor Workflow

To understand the overall TGDetect workflow and how monitors fit into the overall work process, see Use TGDetect.

Monitor Interface

To work with monitors, access the Work with Monitors interface.

To access the Work with Monitors interface

1) Log into to TGDetect. The Main menu appears.
2) At the Selection or command prompt, enter 1 (Working with Monitors).
3) Press Enter. The Work with Monitors interface is displayed.

See also

Monitors
Display Monitors

Use this task to do the following with monitors:

- Display List
- Move to Position in List

Display List

Use this task to display the list of monitors.

To display the list of monitors

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 1 (Working with Monitors).
3) Press Enter. The Work with Monitors interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Name</td>
<td>Object to be monitored</td>
</tr>
<tr>
<td>Monitor Lib</td>
<td>Library to be monitored</td>
</tr>
<tr>
<td>Type</td>
<td>Type of monitor:</td>
</tr>
<tr>
<td></td>
<td>*CMD - Command monitor</td>
</tr>
<tr>
<td></td>
<td>*JRN - Journal monitor</td>
</tr>
<tr>
<td></td>
<td>*MSGQ - Message queue monitor</td>
</tr>
<tr>
<td></td>
<td>*QHST - History log monitor</td>
</tr>
<tr>
<td></td>
<td>*SIEM - Journal archival monitor (used for batch jobs)</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the monitor</td>
</tr>
<tr>
<td>Protect</td>
<td>Whether monitor is internal (built-in):</td>
</tr>
<tr>
<td></td>
<td>Y - Internal (cannot be deleted)</td>
</tr>
<tr>
<td></td>
<td>N - Custom (can be deleted)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Internal monitors are shipped with the product and cannot be deleted compare to custom message queue monitors which can be deleted.</td>
</tr>
<tr>
<td>Status</td>
<td>Whether monitoring is enabled:</td>
</tr>
<tr>
<td></td>
<td>*ACTIVE - Monitor is enabled</td>
</tr>
<tr>
<td></td>
<td>*INACTIVE - Monitor is disabled</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Only active monitors collect data for notifications purposes.</td>
</tr>
<tr>
<td>Daily Alerts</td>
<td>Number of daily alerts triggered</td>
</tr>
<tr>
<td>Monthly Alerts</td>
<td>Number of monthly alerts triggered</td>
</tr>
</tbody>
</table>
Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **User** column so that column heading initially appears in white text.

**To sort the list**

1) Access the **Work with Monitors** interface.

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with Monitors** interface.

2) Sort the list based on the desired column heading.

3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.

4) Press **Enter**. The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**See also**

- Working with Monitors
- Manage Monitors
Manage Monitors

Use this task to do the following:

- Add Monitor
- Start Monitor From Last Processing Time
- Start Monitor From Current Time
- End Monitor
- Delete Monitor

Tip: To manage monitors, access from the Work with Monitors interface.

Access the Work with Monitor Interface

To access the Work with Monitors interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 1 (Working with Monitors).
3) Press Enter. The Work with Monitors interface is displayed.

Add Monitor

Use this task to add a monitor. Once enabled (started) the monitor will begin collecting information for use in notifications.

Tip: Monitoring must be started (enabled) to produce notifications.

Note: At this time, you can add custom message queue monitors only. Each user has their own individual message queue that displays messages specific to the user.

To add a monitor

1) Access the Work with Monitors interface.
2) Press the F6 (Add Monitor) function key. The Work with Monitor - Add record interface is displayed.
3) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Name</td>
<td>Name of the object you want to monitor</td>
</tr>
<tr>
<td>Monitor Library</td>
<td>Library you want to monitor</td>
</tr>
<tr>
<td>Type</td>
<td>*MSGQ - Message queue monitor</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Note</td>
<td>At this time, you can add custom message queue monitors only. Each user has their own individual message queue that displays messages specific to the user.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description identifying the purpose of the monitor</td>
</tr>
</tbody>
</table>

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

**Start Monitor From Last Processing Time**

Use this task to enable monitoring beginning at the last processing time.

Tip: This option is useful if, for example, the monitor was mistakenly disabled or shut down for a week. Therefore, you want to collect data from the last known processing time (not the current time).

Once enabled, the monitor will begin doing the following:

- Collecting information
- Evaluating activities to established monitoring rules
- Sending alerts (notifications)

Tip: Monitoring must be started (enabled) to produce notifications.

**To start monitoring from the last processing time**

1) Access the **Work with Monitor** interface.
2) In the **OPT** column for the desired monitor, enter 1 (Start Monitor).
3) Press Enter twice. Monitors that you enabled (started) should appear with a status of *ACTIVE*.

**Start Monitor From Current Time**

Use this task to enable monitoring beginning at the current time (not the last known process time).

Once enabled, the monitor will begin doing the following:

- Collecting information
- Evaluating activities to established monitoring rules
- Sending alerts (notifications)

Tip: Monitoring must be started (enabled) to produce notifications.

**To start monitoring from the current time**

1) Access the **Work with Monitor** interface.
2) In the OPT column for the desired monitor, enter 21 (Start Monitor Current Time).

3) Press Enter twice. Monitors that you enabled (started) should appear with a status of *ACTIVE.*

**End Monitor**

Use this task to disable a monitor.

**To start monitoring**

1) Access the Work with Monitor interface.

2) In the OPT column for the desired monitor, enter 2 (End Monitor).

3) Press Enter twice. Monitors that you disabled (ended) should appear with a status of *INACTIVE.*

**Delete Monitor**

Use this task to delete a monitor.

**To delete a monitoring**

1) Access the Work with Monitors interface.

2) In the OPT column for the desired requirement, enter 4 (Delete).

3) Press Enter.

4) Review the record to ensure you are deleting the correct requirement.

5) Press Enter twice.

**See also**

Log Into TGDetect

Working with Monitors
Run Monitor Master Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run Monitor Master Report
- Run All Activity Report

⚠️ Note: Refer to the TGDetect Report Reference for a complete list of report definitions.

✅ Tip: To run monitor reports, access from the TGDetect Reports interface.

Access the TGDetect Reports Interface

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TGDetect Reports interface is displayed.

Run Monitor Master Report

Use this report to display the list of monitors (built-in and custom).

To run the Monitor Master Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 2 (Configuration Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 2 (Monitor Master).
5) Press Enter.
6) Modify the run criteria as necessary.

⚠️ Note: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

✅ Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the Report output type field.
8) Press Enter. The status of the report is displayed at the bottom of the screen.
Run All Activity Report

Use this report to display all history activity (QHST, QSYSOPR, etc.).

To run the All History Activity Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 1 (Activity History Reports).
3) Press Enter. The TGDetect Reports interface is displayed.
4) At the Selection or command prompt, enter 1 (All History Activity).
5) Press Enter.
6) Modify the run criteria as necessary.

**Note:** The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

**Tip:** Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the Report output type field.
8) Press Enter. The status of the report is displayed at the bottom of the screen.

See also

Working with Monitors

Working with Reports
Command Monitor

This section describes working with Command (CMD) Monitor.

This section includes the following topics:

- Working with Command Monitor
- Display Command Monitor Rules
- Display Command Monitor Rule Criteria
- Display Command Monitor Alerts
- Display Command Monitor Activity Log
- Manage Command Monitor Rules
- Manage Command Monitor Rule Criteria
- Manage Command Monitor Alerts
- Run Command Monitor Reports

See also

Monitors
Working with Command Monitor

Use the Command Monitor to do the following:

- Display Command Monitor Rule Criteria
- Display Command Monitor Alerts
- Display Command Monitor Activity Log
- Manage Command Monitor Rules
- Manage Command Monitor Rule Criteria
- Manage Command Monitor Alerts
- Run Command Monitor Reports

Tip: To work with the Command Monitor, you must access the Work with Monitors interface.

To access the Work with Monitors interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 1 (Working with Monitors).
3) Press Enter. The Work with Monitors interface is displayed.

See also

Command Monitor
Display Command Monitor Rules

Use this task to do the following with command monitor rules:

- Display List
- Filter List

Display List

Use this task to display the list of command monitor rules.

To display the list of command monitor rules

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 5 (Command Monitor Rules).


<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique Identifier assigned to command rule</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Name of the calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td>Daily Count</td>
<td>Number of daily alerts triggered by rule</td>
</tr>
<tr>
<td>Note:</td>
<td>The count is reset each time a new alert is triggered. In other words, if</td>
</tr>
<tr>
<td></td>
<td>three alerts were triggered on a Monday, and you displayed this interface</td>
</tr>
<tr>
<td></td>
<td>at the end of the day on Monday, this field would display the number 3. If</td>
</tr>
<tr>
<td></td>
<td>no alerts were triggered on Tuesday, and you accessed this interface at the</td>
</tr>
<tr>
<td></td>
<td>end of day on Tuesday, the value would still display the number 3 because</td>
</tr>
<tr>
<td></td>
<td>no new alerts were triggered. If a single alert were triggered on Wednesday,</td>
</tr>
<tr>
<td></td>
<td>and you accessed this interface at end of day on Wednesday, the value would</td>
</tr>
<tr>
<td></td>
<td>then display the number 1. The value 1 would display in this field until a</td>
</tr>
<tr>
<td></td>
<td>new alert is triggered.</td>
</tr>
<tr>
<td>Monthly Count</td>
<td>Number of monthly alerts triggered by rule</td>
</tr>
<tr>
<td>Yearly Count</td>
<td>Number of yearly alerts triggered by rule</td>
</tr>
</tbody>
</table>

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Rules - CMD interface.
2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Filter List**

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.
- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules - CMD** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with Command Monitor Rules*

*Manage Command Monitor Rules*
Display Command Monitor Rule Criteria

Use this task to do the following with command monitor rule criteria:

- Display List
- Filter List

Display List

Use this task to display the list of command monitor rule criteria

To display the list of command monitor rule criteria

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 5 (Command Monitor Rules).


4) In the OPT column for the desired command monitor rule, enter 10 (Rule Criteria). The Work with Rule Criteria - CMD interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Command Name</td>
<td>Command for which you want to establish a rule</td>
</tr>
<tr>
<td>Command Library</td>
<td>Library in which you want to monitor using the rule</td>
</tr>
<tr>
<td>User Name</td>
<td>User/user group you want to monitor using the rule</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Enter <em>ALL</em> to monitor all users.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the criteria</td>
</tr>
</tbody>
</table>

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list

1) Access the Work with Rules - CMD interface.

2) Place your cursor on the desired column heading.

3) Press the F10 (Sort) function key on your keyboard.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.
To filter the list using a subset

1) Access the **Work with Rules - CMD** interface.

2) Press the **F8** (Subset) function key on your keyboard.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

- Working with Command Monitor Rules
- Manage Command Monitor Rule Criteria

---

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.
Display Command Monitor Alerts

Use this task to display the list of alerts available for use with the command monitor. Command monitor alerts (notifications) are the messages sent when the criteria established for a command monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system that needs to take action).

To display the list of command monitor alerts

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 5 (Command Monitor Rules).


4) In the Opt column for the desired rule, enter 20 (Alerts). The Work with Alert - CMDMON interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying alerts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule for which you are displaying alerts</td>
</tr>
<tr>
<td>Alt Seq</td>
<td>The sequence in which alerts are sent</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Type of alert</td>
</tr>
<tr>
<td><em>EMAIL</em></td>
<td>Send an email alert to a specific user/group</td>
</tr>
<tr>
<td><em>MSG</em></td>
<td>Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td><em>CMD</em></td>
<td>Execute a command</td>
</tr>
<tr>
<td><em>SYSLOG</em></td>
<td>Send a notification to the system archive</td>
</tr>
<tr>
<td><em>EMAILDIST</em></td>
<td>Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td><em>TGCENTRAL</em></td>
<td>Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Details</td>
<td>Recipient details</td>
</tr>
<tr>
<td>Message to Send</td>
<td>Text included in the notification sent to the designated recipient</td>
</tr>
<tr>
<td>Alert Criteria - #Events</td>
<td>Number of alert events required to trigger a notification</td>
</tr>
<tr>
<td>Alternatively, enter <em>ALL</em> to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Freq field.</td>
<td></td>
</tr>
<tr>
<td>Alert Criteria - Freq</td>
<td>Frequency of alert events required to trigger a notification</td>
</tr>
<tr>
<td>This field works in conjunction with the #Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.</td>
<td></td>
</tr>
</tbody>
</table>

See also
Working with Command Monitor Rules

Manage Command Monitor Alerts
Display Command Monitor Activity Log

Use this task to display the list of triggered notifications (alerts) produced from the command monitor. Command monitor alerts are the messages sent when the criteria established for a command monitor rule are met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system).

Tip: The command monitor activity log displays all activity types (i.e., CMD, *EMAIL, *MSG, *SYSLOG, *TGCENTRAL). If you want to filter the list to display only a specific activity type, use the *F8 keyboard function to create a subset. Alternatively, you can access the activity log via a specific monitor type to see only activities associated with that monitor type. For example, access the activity log via the history log monitor to see only *MSG activities or the message queue activity log via the message queue monitor to see only *EMAIL activities.

To display the command monitor activity log

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 5 (Command Monitor Rules).
4) In the Opt column for the desired history log rule, enter 30 (Work with Activity). The Work with Activity - CMDMON interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying activity</td>
</tr>
<tr>
<td>Activity Type</td>
<td>Type of alert:</td>
</tr>
<tr>
<td></td>
<td>*CMD - Command executed</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Email sent</td>
</tr>
<tr>
<td></td>
<td>*MSG - System (login) message queued</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Syslog communication initiated</td>
</tr>
<tr>
<td>Activity Status</td>
<td>Status of alert</td>
</tr>
<tr>
<td>Activity Date</td>
<td>Date on which the alert was triggered</td>
</tr>
<tr>
<td>Activity Time</td>
<td>Time at which the alert was triggered</td>
</tr>
<tr>
<td>Activity Details</td>
<td>Description of alert</td>
</tr>
</tbody>
</table>

See also

- Working with Command Monitor Rules
- Working with Monitor Activity Logs
Manage Command Monitor Rules

Use this task to do the following:

- Access Work with Rules - CMDMON Interface
- Add Command Monitor Rule
- Edit Command Monitor Rule
- Edit Command Monitor Rule Criteria
- Edit Command Monitor Alerts
- Delete Command Monitor Rule

Tip: To manage the command monitors rules, access from the Work with Rules - CMDMON interface.

Access Work with Rules - CMDMON Interface

To access the Work with Rules - CMD interface
1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 5 (Command Monitor Rules).

Add Command Monitor Rule

Use this task to add a command monitor rule.

To add a command monitor rule
1) Access the Work with Rules - CMDMON interface.
2) Press the F6 (Add) function key on your keyboard. The Work with Rules - Add.
3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Enter a unique identifier for the command rule</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Enter a name for the command rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the name of the calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td></td>
<td>Tip: Enter *NONE if no calendar is applicable.</td>
</tr>
</tbody>
</table>

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

Edit Command Monitor Rule
Use this task to edit a command monitor rule.

To edit command monitor rule
1) Access the Work with Rules - CMDMON interface.
2) In the Opt column for the desired command monitor rule, enter 2 (Change).
3) Press Enter.
4) Modify the parameters as necessary.
5) Press Enter twice.

Edit Command Monitor Rule Criteria
See Manage Command Monitor Rule Criteria.

Edit Command Monitor Alerts
See Manage Command Monitor Alerts.

Delete Command Monitor Rule
Use this task to delete a command monitor rule.

To delete a command monitor rule
1) Access the Work with Rules - CMDMON interface.
2) In the Opt column for the desired command monitor rule, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct command monitor rule.
5) Press Enter twice.

See also
Working with Command Monitor Rules
Display Command Monitor Rules
Manage Command Monitor Rule Criteria

Use this task to do the following:

- Access Work with Rule Criteria - CMD interface
- Add Rule Criteria
- Edit Rule Criteria
- Delete Rule Criteria

Tip: To manage the command monitors rule criteria, access from the Work with Rule Criteria - CMD interface.

Access Work with Rule Criteria - CMD interface

To access the Work with Rule Criteria - CMD interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 5 (Command Monitor Rules).
4) In the OPT column for the desired command monitor rule, enter 10 (Rule Criteria). The Work with Rule Criteria - CMD interface is displayed.

Add Rule Criteria

Use this task to add command monitor rule criteria.

To add rule criteria

1) Access the Work with Rule Criteria - CMD interface.
2) Press the F6 (Add) function key on your keyboard. The Work with Rule Criteria - Add interface is displayed.
3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Name</td>
<td>Enter the command for which you want to establish a rule</td>
</tr>
<tr>
<td>Command Library</td>
<td>Enter the library in which you want to monitor using the rule</td>
</tr>
<tr>
<td>Command User</td>
<td>Enter the user/user group you want to monitor using the rule</td>
</tr>
<tr>
<td></td>
<td>Tip: Enter *ALL to monitor all users.</td>
</tr>
</tbody>
</table>

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.
Edit Rule Criteria

Use this task to edit the command monitor rule criteria

To edit rule criteria

1) Access the Work with Rule Criteria - CMD interface.
2) In the OPT column for the desired rule criteria, enter 2 (Change).
3) Press Enter.
4) Modify the parameters as necessary.
5) Press Enter twice.

Delete Rule Criteria

Use this task to delete a command monitor rule criteria.

To delete rule criteria

1) Access the Work with Rule Criteria - CMD interface.
2) In the OPT column for the desired rule criteria, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct rule criteria.
5) Press Enter twice.

See also

Working with Command Monitor Rules
Display Command Monitor Rule Criteria
Manage Command Monitor Alerts

Use this task to do the following:

- Access Work with Alert - CMDMON Interface
- Add Alert
- Edit Alert
- Delete Alert

Tip: To manage the history log alerts, access from the Work with Alert - CMDMON interface.

Access Work with Alert - CMDMON Interface

To access the Work with Alerts - CMDMON interface

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 5 (Command Monitor Rules).


4) In the OPT column for the desired history log rule, enter 20 (Alert). The Work with Alert - CMDMON interface is displayed.

Add Alert

Use this task to add a command monitor alert.

To add alert

1) Access the Work with Alert - CMDMON interface.

2) Press the F6 (Add) function key on your keyboard. The Add Alert - CMDMON interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Type</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Send an email alert to a specific user/group</td>
</tr>
<tr>
<td></td>
<td>*MSG - Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td></td>
<td>*CMD - Execute a command</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Send a notification to the system archive</td>
</tr>
<tr>
<td></td>
<td>*EMAILDIST - Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td></td>
<td>*TGCENTRAL - Send a notification to TGCentral</td>
</tr>
</tbody>
</table>

Alert Sequence | Enter the sequence in which you want alerts sent. Note: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.

Alert Message | Enter the text you want to be included in the notification sent to the designated recipient.
Enter the number of alert events required to trigger a notification. Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Event Frequency field.

Enter the frequency of alert events required to trigger a notification. This field works in conjunction with the Number of Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.

Enter the frequency unit:
- DAYS - Days
- HR - Hours
- MIN - Minutes
- SEC - Second

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

Edit Alert

Use this task to edit a command monitor alert.

To edit alert
1) Access the Work with Alert - CMDMON interface.
2) In the OPT column for the desired rule criteria, enter 2 (Change).
3) Press Enter.
4) Modify the parameters as necessary.
5) Press Enter twice.

Delete Alert

Use this task to delete a command monitor alert.

To delete alert
1) Access the Work with Alert - CMDMON interface.
2) In the OPT column for the desired rule criteria, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct alert.
5) Press Enter twice.

See also
Working with Command Monitor Rules

Display Command Monitor Alerts
Run Command Monitor Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run Command Monitor Alert Report
- Run Command Monitor Alert Change Report
- Run Command Monitor Rule Report
- Run Command Monitor Rule Change Report

Tip: Refer to the TGDetect Report Reference for a complete list of report definitions.

Note: To work with default setting reports, access from the TGDetect Reports interface.

Access the TGDetect Reports Interface

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TGDetect Reports interface is displayed.

Run Command Monitor Activity Report

Use this report to display the list of command monitor activities.

To run the Command Monitor Activity Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 1 (Activity History Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 4 (Command Monitor Activity).
5) Press Enter.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Command Monitor Alert Report
Use this report to display the list of command monitor alerts.

**To run the Command Monitor Alert Report**

1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 2 (Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 6 (Message Queue and Command Alerts).

5) Press **Enter**.

6) Modify the run criteria as necessary.

---

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

**Tip**: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Command Monitor Alert Change Report**

Use this report to display the list of command monitor alert changes.

**Tip**: Auditing must be enabled to run change reports. See Add Auditing Defaults for a list of reports available.

**To run Command Monitor Alert Change Report**

1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Change Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 5 (Msg Queue and Command Alerts Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

---

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

**Tip**: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.
7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Command Monitor Rule Report**

Use this report to display the list of command monitor rules.

**To run the Command Monitor Rule Report**

1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 2 (Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 5 (Command Monitor Rules).

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Note**: The criteria allow you to limit the data returned in the report. To see field descriptions of common report criteria, see Run Reports.

**Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Command Monitor Rule Change Report**

Use this report to display the list command monitor rule header changes.

**Tip**: Auditing must be enabled to run change reports. See *Add Auditing Defaults* for a list of reports available.

**To run Command Monitor Change Report**

1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Change Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 6 (Cmd Monitor Rules Header Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.
7) Enter the desired output format in the **Report output type** field.

8) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

*Working with Command Monitor Rules*

*Working with Monitor Reports*
History Log Monitor

This section describes working with History Log (QHST) Monitor:

- Working with History Log Monitor
- Display History Log Rules
- Display History Log Rule Criteria
- Display History Log Alerts
- Display History Log Activity Log
- Manage History Log Rules
- Manage History Log Rule Criteria
- Manage History Log Alerts
- Run History Log Reports

See also

Monitors
Working with History Log Monitor

Use the History Log (QHST) monitor to do the following:

- Display History Log Rules
- Display History Log Rule Criteria
- Display History Log Alerts
- Display History Log Activity Log
- Manage History Log Rules
- Manage History Log Rule Criteria
- Manage History Log Alerts
- Run History Log Reports

Tip: To work with the History Log Monitor, you must access the Work with Monitors interface.

To access the Work with Monitors interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 1 (Working with Monitors).
3) Press Enter. The Work with Monitors interface is displayed.

See also

History Log Monitor
Display History Log Rules

Use this task to do the following with QHST history log rules:

- Display List
- Filter List

Display List

Use this task to display the list of history log monitor rules.

To display the list of history log rules

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 2 (History Log Rules).

3) Press Enter. The Work with Rules interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique Identifier assigned to history log rule</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See History Log Rules for a description of the built-in rules that ship with TGDetect.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Name of the calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td>Daily Count</td>
<td>Number of daily alerts triggered by rule</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered.</td>
</tr>
<tr>
<td>Monthly Count</td>
<td>Number of monthly alerts triggered by rule</td>
</tr>
<tr>
<td>Yearly Count</td>
<td>Number of yearly alerts triggered by rule</td>
</tr>
</tbody>
</table>

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list
1) Access the **Work with Rules** interface.

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

### Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

- **Working with History Log Rules**
- **Manage History Log Rules**
Display History Log Rule Criteria

Use this task to do the following with QHST history log rule criteria:

- Display List
- Filter List

Display List

Use this task to display the list of history log rule criteria.

To display the list of history log rule criteria

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 2 (History Log Rules).
4) In the OPT column for the desired history log rule, enter 10 (Rule Criteria). The Work with Rule Criteria - QSYS/QHST interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Minimum Severity</td>
<td>The rule severity level that must be met to trigger a message (notification)</td>
</tr>
<tr>
<td>MSGID</td>
<td>Unique ID assigned to the message rule criteria</td>
</tr>
<tr>
<td>Message File</td>
<td>File in which the message rule resides</td>
</tr>
<tr>
<td>Message Library</td>
<td>Library in which the message rule resides</td>
</tr>
<tr>
<td>Description</td>
<td>Description of rule</td>
</tr>
<tr>
<td>Omit or Select</td>
<td>Identifies whether the rule criteria is used for selecting or omitting:</td>
</tr>
<tr>
<td></td>
<td>S (Select) - Rule criteria used to identify messages to include (trigger alerts)</td>
</tr>
<tr>
<td></td>
<td>O (Omit) - Rule criteria used to identify messages to exclude (should not trigger alerts)</td>
</tr>
<tr>
<td>Field Compare</td>
<td>Identifies any field value filters</td>
</tr>
<tr>
<td>Reply</td>
<td>Reply sent to the recipient</td>
</tr>
</tbody>
</table>

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

### Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report*) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules - QSYS/QHST** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

- Working with History Log Rules
- Manage History Log Rule Criteria
Display History Log Alerts

Use this task to display the list of alerts available for use with the QHST history log. History log alerts are the messages (notifications) sent when the criteria established for a history log monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system that needs to take action).

To display history log alerts

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 2 (History Log Rules).

3) Press Enter. The Work with Rules interface is displayed.

4) In the OPT column for the desired history log rule, enter 20 (Alerts). The Work with Alert - QSYS/QHST interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying alerts</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule for which you are displaying alerts</td>
</tr>
<tr>
<td>Alt Seq</td>
<td>The sequence in which alerts are sent</td>
</tr>
<tr>
<td>Note: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.</td>
<td></td>
</tr>
<tr>
<td>Alert Type</td>
<td>Type of alert</td>
</tr>
<tr>
<td>*EMAIL</td>
<td>- Send an email alert to a specific user/group</td>
</tr>
<tr>
<td>*MSG</td>
<td>- Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td>*CMD</td>
<td>- Execute a command</td>
</tr>
<tr>
<td>*SYSLOG</td>
<td>- Send a notification to the system archive</td>
</tr>
<tr>
<td>*EMAILDIST</td>
<td>- Send an email alert to a specific user/group (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td>*TGCENTRAL</td>
<td>- Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Details</td>
<td>Recipient details</td>
</tr>
<tr>
<td>Message to Send</td>
<td>Text included in the notification sent to the designated recipient</td>
</tr>
<tr>
<td>Alert Criteria - #Events</td>
<td>Number of alert events required to trigger a notification</td>
</tr>
<tr>
<td>Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Freq field.</td>
<td></td>
</tr>
<tr>
<td>Alert Criteria - Freq</td>
<td>Frequency of alert events required to trigger a notification</td>
</tr>
<tr>
<td>This field works in conjunction with the #Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.</td>
<td></td>
</tr>
</tbody>
</table>
See also

- Working with History Log Rules
- Manage History Log Alerts
Display History Log Activity Log

Use this task to display the list of triggered notifications (alerts) produced from the QHST history log. History log alerts are the messages sent when the criteria established for a history log monitor rule is met. In other words, when the criteria established for a rule is met, the system sends system message (*MSG) alert to a designated recipient (user, user group, or system that needs to take action).

To display history log activity log

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 2 (History Log Rules).

3) Press Enter. The Work with Rules interface is displayed.

4) In the OPT column for the desired history log rule, enter 30 (Work with Activity). The Work with Activity - QSYS/QHST interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying activity</td>
</tr>
<tr>
<td>Activity Type</td>
<td>Type of alert:</td>
</tr>
<tr>
<td></td>
<td>*MSG - System (login) message queued</td>
</tr>
<tr>
<td>Activity Status</td>
<td>Status of alert</td>
</tr>
<tr>
<td>Activity Date</td>
<td>Date on which the alert was triggered</td>
</tr>
<tr>
<td>Activity Time</td>
<td>Time at which the alert was triggered</td>
</tr>
<tr>
<td>Activity Details</td>
<td>Description of activity</td>
</tr>
</tbody>
</table>

See also

Working with History Log Rules

Working with Monitor Activity Logs
Manage History Log Rules

Use this task to do the following:

- Access the Work with Rules - QSYS/QHST Interface
- Add History Log Rule
- Edit History Log Rule
- Edit History Log Rule Criteria
- Edit History Log Alerts
- Delete History Log Rule

Tip: To manage the history log rules, access from the Work with Rules interface.

Access the Work with Rules - QSYS/QHST Interface

To access the Working with Rules interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 2 (History Log Rules).

Add History Log Rule

Use this task to add a history log rule.

To add a history rule

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Enter a unique identifier for the history log rule</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Enter a name for the history log rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the name of the calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td></td>
<td>Tip: Enter *NONE if no calendar is applicable.</td>
</tr>
</tbody>
</table>

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

Edit History Log Rule

Trinity Guard
Use this task to edit a history log rule.

**To edit a history log rule**

1) Access the **Work with Rules - QSYS/QHST** interface.
2) In the **OPT** column for the desired history log rule, enter 2 (Change).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

**Edit History Log Rule Criteria**

See [Manage History Log Rule Criteria](#).

**Edit History Log Alerts**

See [Manage History Log Alerts](#).

**Delete History Log Rule**

Use this task to delete a history log rule.

**To delete a history log rule**

1) Access the **Work with Rules - QSYS/QHST** interface.
2) In the **OPT** column for the desired history log rule, enter 4 (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct history log rule.
5) Press **Enter** twice.

**See also**

[Working with History Log Rules](#)

[APPENDIX - TGDetect Built-in History Log (QHST) Rules](#)
Manage History Log Rule Criteria

Use this task to do the following:

- Access Work with Rule Criteria - QSYS/QHST interface
- Add Rule Criteria
- Delete Rule Criteria
- Edit Rule Criteria
- Compare Fields
- Add Reply
- Limit Notifications to Messages that Require a Reply
- Change Severity

Tip: To manage the history log rule criteria, access from the Work with Rule Criteria - QSYS/QHST interface.

Access Work with Rule Criteria - QSYS/QHST interface

To access the Work with Rule Criteria - QSYS/QHST interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 2 (History Log Rules).
3) Press Enter. The Work with Rules interface is displayed.
4) In the OPT column for the desired history log rule, enter 10 (Rule Criteria). The Work with Rule Criteria - QSYS/QHST interface is displayed.

Add Rule Criteria

Use this task to add history log rule criteria.

To add rule criteria

1) Access the Work with Rule Criteria - QSYS/QHST interface.
2) Press the F6 (Add) function key. The Work with Rule Criteria - Add interface is displayed
3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message ID</td>
<td>Enter a unique ID for the message rule</td>
</tr>
<tr>
<td>Message File</td>
<td>Enter the file in which the message rule resides</td>
</tr>
<tr>
<td>Message File Library</td>
<td>Enter the library in which the message rule resides</td>
</tr>
</tbody>
</table>
| Message Omit or Select | Enter whether the rule is used for selecting or omitting:  
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| S (Select)            | Rule criteria used to identify messages to include (trigger alerts)  
| O (Omit)              | Rule criteria used to identify messages to exclude (should not trigger alerts)  

| Message Reply | Identifies whether a reply exists. Some actions require a reply in order to execute a follow-up action.  
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Note: This allows you to set up the required reply to ensure that the workflow is not hindered. |

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

**Delete Rule Criteria**

Use this task to delete history log rule criteria.

To delete rule criteria

1) Access the Work with Rule Criteria - QSYS/QHST interface.
2) In the OPT column for the desired rule criteria, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct rule criteria.
5) Press Enter twice.

**Edit Rule Criteria**

Use this task to edit history log rule criteria.

To edit rule criteria

1) Access the Work with Rule Criteria - QSYS/QHST interface.
2) In the OPT column for the desired rule criteria, enter 2 (Change).
3) Press Enter.
4) Modify the parameters as necessary.
5) Press Enter twice.

**Compare Fields**

Use this task to add additional filtering criteria specific to field values.

Note: This feature allows you to apply additional granularity to your monitor rules and to further limit alert notifications.
To compare fields

1) Access the Work with Rule Criteria - QSYS/QHST interface.
2) In the OPT column for the desired rule criteria, enter 10 (Field Compare).
3) Press Enter.
4) Place your cursor in the first available (blank) Opt column field and press the F4 (Select Fields) function key on your keyboard.

Note: The list of field(s) that you can use for comparison are displayed in a Selection dialog. The selections available in the dialog should match the variable fields that appear with an & placeholder in the message description.

Tip: If the dialog contains no compare fields (blank), then this feature is not available for the selected message.

5) Enter 1 in the Sel column for the field(s) you want to use in your filter.
6) Press Enter.
7) Enter the field-specific criteria you want to use to filter alert notifications.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press the F10 function key on your keyboard.

Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis “(“ in the Nest Str column. Likewise, to end a nested condition, enter a closing parenthesis “)” in the Nest End column.

8) Press Enter.

Add Reply

Use this task to create replies. Some actions require a reply (an answer to a question) in order to proceed.
**Note**: This feature allows you to set up a required reply in anticipation of this type of request to ensure that the workflow is not hindered.

**To create replies**

1) Access the **Work with Rule Criteria - QSYS/QHST** interface.

2) In the **OPT** column for the desired rule criteria, enter **20** (Work with Reply).

3) Press **Enter**.

4) Enter the necessary reply.

5) Press **Enter**.

**Limit Notifications to Messages that Require a Reply**

Use this task when you want to limit message notification to only messages in a message queue that require a reply (C G D F).

**To limit Notification to only messages that require a reply**

1) Access the **Work with Rule Criteria - QSYS/QHST** interface.

2) Press the **F9** (Monitor MSGs Need Reply Only) function key. The **Work with Rule Criteria - Monitor MSGs Need Reply Only** interface is displayed.

3) Modify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Messages Requiring Reply Only</td>
<td>Enter one of the following:</td>
</tr>
<tr>
<td></td>
<td>*NO - Send notifications for all message in the queue</td>
</tr>
<tr>
<td></td>
<td>*YES - Send notifications for only messages that required a reply</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong>: To see the complete list of messages present in a message queue (those that required a reply and those that do not), use the command <strong>DSPMSG</strong>.</td>
</tr>
</tbody>
</table>

4) Press **Enter**.

**Change Severity**

Use this task when you want to limit message notification by severity level. By default, the severity minimum is set to zero (00), which includes all severity levels. For example, if you want to exclude 00 (informational) messages from the notifications you receive, then change the minimum severity level to 20 (Error).

**Tip**: The severity scale (00-99) is based on IBM limits. See the IBM Knowledge Base for documentation on severity levels.
To change the minimum severity

1) Access the **Work with Rule Criteria - QSYS/QHST** interface.

2) Press the **F7 (Change Severity)** function key. The **Work with Rule Criteria - Change Severity** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Minimum Severity  | Enter the minimum severity level required:  
|                   | 00 - Information.  
|                   | 20 - Error  
|                   | 30 - Severe error  
|                   | 40 - Abnormal end of procedure or function  
|                   | 50 - Abnormal end of job  
|                   | 60 - System status  
|                   | 70 - Device integrity  
|                   | 80 - System alert  
|                   | 90 - System integrity  
|                   | 99 - Action                                                                                                                                 |

4) Press **Enter**.

**See also**

- **Working with History Log Rules**
- **Display History Log Rule Criteria**
Manage History Log Alerts

Use this task to do the following:

- Access Work with Alert - QSYS/QHST interface
- Edit Alert
- Delete Alert

Tip: To manage the history log alerts, access from the Work with Alert - QSYS/QHST interface.

Access Work with Alert - QSYS/QHST interface

To access the Work with Alert - QSYS/QHST interface

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 2 (History Log Rules).

3) Press Enter. The Work with Rules interface is displayed.

4) In the OPT column for the desired history log rule, enter 20 (Alert). The Work with Alert - QSYS/QHST interface is displayed.

Add Alert

Use this task to add a history log alert.

To add alert

1) Access the Work with Alert - QSYS/QHST interface.

2) Press the F6 (Add) function key. The Add Alert - QSYS/QHST interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Type</td>
<td>Enter one of the following options: <em>EMAIL</em> - Send an email alert to a specific user/group <em>MSG</em> - Send a system message (message that appears when a user logs into the system) <em>CMD</em> - Execute a command <em>SYSLOG</em> - Send a notification to the system archive <em>EMAILDIST</em> - Send an email alert to a specific user (legacy IBM method of sending email alerts) <em>TGCENTRAL</em> - Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Sequence</td>
<td>Enter the sequence in which you want alerts sent <strong>Note:</strong> You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.</td>
</tr>
<tr>
<td>Alert Message</td>
<td>Enter the text you want to be included in the notification sent to the designated recipient</td>
</tr>
<tr>
<td><strong>Number of Events</strong></td>
<td>Enter the number of alert events required to trigger a notification. Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the <strong>Event Frequency</strong> field.</td>
</tr>
<tr>
<td><strong>Event Frequency</strong></td>
<td>Enter the frequency of alert events required to trigger a notification. This field works in conjunction with the <strong>Number of Events</strong> field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period. <strong>Tip:</strong> This option is useful for setting thresholds that must be met before an alert is triggered.</td>
</tr>
<tr>
<td><strong>Event</strong></td>
<td>Enter the frequency unit: DAYS - Days HR - Hours MIN - Minutes SEC - Second</td>
</tr>
</tbody>
</table>

**Tip:** Press F1 (Help) to access field descriptions.

4) Press **Enter** twice.

**Edit Alert**

Use this task to edit a history log alert.

**To edit alert**

1) Access the Work with Alert - QSYS/QHST interface.
2) In the **OPT** column for the desired rule criteria, enter **2** (Change).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

**Delete Alert**

Use this task to delete a history log alert.

**To delete alert**

1) Access the Work with Alert - QSYS/QHST interface.
2) In the **OPT** column for the desired rule criteria, enter **4** (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct alert.
5) Press **Enter** twice.

**See also**
Working with History Log Rules

Display History Log Alerts
Run History Log Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run History Log Activity Report

Tip: Refer to the TGDetect Report Reference for a complete list of report definitions.

Note: To work with default setting reports, access from the TGDetect Reports interface.

Access the TGDetect Reports Interface

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TGDetect Reports interface is displayed.

Run History Log Activity Report

Use this report to display the list of history activities (QHST only).

To run the History Log Activity Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 1 (Activity History Reports).
3) Press Enter. The TGDetect Reports interface is displayed.
4) At the Selection or command prompt, enter 2 (History Log Activity).
5) Press Enter.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

See also

Working with History Log Rules
Working with Monitor Reports
Journal Monitor

This section describes working with **Journal (JRN) Monitor**:

- Working with Journal Monitor
- Display Journal Monitor Rules
- Display Journal Monitor Rule Criteria
- Display Journal Monitor Alerts
- Display Journal Monitor Activity Log
- Manage Journal Monitor Rules
- Manage Journal Monitor Rule Criteria
- Manage Journal Monitor Alerts
- Run Journal Monitor Reports

**See also**

Monitors
Working with Journal Monitor

Use the **Journal (JRN) Monitor** to do the following:

- Display Journal Monitor Rules
- Display Journal Monitor Rule Criteria
- Display Journal Monitor Alerts
- Display Journal Monitor Activity Log
- Manage Journal Monitor Rules
- Manage Journal Monitor Rule Criteria
- Manage Journal Monitor Alerts
- Run Journal Monitor Reports

**Tip**: To work with the Journal Monitor, you must access the **Work with Monitors** interface.

To access the **Work with Monitors** interface

1) Access the TGDetect **Main** menu.

2) At the **Selection or command** prompt, enter 1 (Working with Monitors).

3) Press **Enter**. The **Work with Monitors** interface is displayed.

**See also**

Journal Monitor
Display Journal Monitor Rules

Use this task to do the following with journal monitor rules:

- **Display List**
- **Filter List**

**Display List**

Use this task to display the list of journal monitor rules.

**To display the list of journal monitor rules**

1) Access the TGDetect **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Journal Monitor Rules).
3) Press **Enter**. The **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alert</strong></td>
<td>Identifies whether an alert is sent:</td>
</tr>
<tr>
<td></td>
<td>Y - Send an alert</td>
</tr>
<tr>
<td></td>
<td>N - Do not send an alert</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To see the SIEM log format in which the system sends alerts, refer to <strong>Manage TGDetect Defaults</strong>.</td>
</tr>
<tr>
<td><strong>Code</strong></td>
<td>Identifies the type of audit trail journal</td>
</tr>
<tr>
<td></td>
<td>The following journal types are currently supported:</td>
</tr>
<tr>
<td></td>
<td>T - Security journal</td>
</tr>
<tr>
<td></td>
<td>U - User-defined journal</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Identifies the type of journal entry</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Refer to the IBM Knowledge Center for a complete list of journal entry types and descriptions.</td>
</tr>
<tr>
<td><strong>Descrip-</strong></td>
<td>Description of the journal entry</td>
</tr>
<tr>
<td><strong>tion</strong></td>
<td><strong>Field Filter</strong> Identifies whether a field-level filter exists</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Field-level filters allow you to apply additional granularity to your monitor rules.</td>
</tr>
<tr>
<td></td>
<td>Y - Field-level filter exists</td>
</tr>
<tr>
<td></td>
<td>N - No field-level filter exists</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To see the filter definition, refer to <strong>Manage SIEM Monitor Rule Criteria</strong>.</td>
</tr>
<tr>
<td><strong>Calendar</strong></td>
<td>Calendar that defines when the rule is applicable</td>
</tr>
</tbody>
</table>
To filter the list using a subset

1) Access the Work with Rules interface.
2) Press the F8 (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press Enter. The system filters the results based on the criteria you defined for the subset.

**Tip:** Use wildcard asterisk to help define your subset.
- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after text to find list items that contain specific text anywhere in the name.

### Filter List

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

<table>
<thead>
<tr>
<th>Daily Count</th>
<th>Number of daily alerts triggered by rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered.</td>
<td></td>
</tr>
<tr>
<td>Monthly Count</td>
<td>Number of monthly alerts triggered by rule</td>
</tr>
<tr>
<td>Yearly Count</td>
<td>Number of yearly alerts triggered by rule</td>
</tr>
</tbody>
</table>

**Sort List**

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

**To sort the list**

1) Access the Work with Rules interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.
See also

Working with Journal Monitor Rules

Manage Journal Monitor Rules
Display Journal Monitor Rule Criteria

Use this task to display field-level filtering criteria.

**Note:** Field filters allow you to apply additional granularity to your monitor rules and to further limit alert notifications.

**To display the list of fields filters**

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter 4 (Journal Monitor Rules).

3) Press **Enter**. The **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface is displayed.

4) Check the **Field Filter** column.

   - If **Y** appears in the column, then a field filter exists for the journal entry type
   - If **N** appears in the column, then a field filter does not exist for the journal entry type

5) In the **Opt** column for a journal entry with a **Y** present in the **Field Filter** column, enter 9 (Filter). The **Work with Filtering Fields** interface is displayed.

**Tip:** If you enter 9 (Filter) in the **Opt** column for a journal entry type with **N** defined, no filters appear. See Manage SIEM Monitor Rule Criteria for instructions on adding field filters.

**See also**

- Working with Journal Monitor Rules
- Manage Journal Monitor Rule Criteria
Display Journal Monitor Alerts

Use this task to display the list of alerts available for use with the journal monitor. Journal monitor log alerts are the messages (notifications) sent when the criteria established for a journal monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system that needs to take action).

To display the list of journal monitor alerts

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 4 (Journal Monitor Rules).


4) In the OPT column for the desired history log rule, enter 20 (Alerts). The Work with Alert - QSYS/QAUDJRN interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt Seq</td>
<td>The sequence in which alerts are sent</td>
</tr>
<tr>
<td></td>
<td>Note: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.</td>
</tr>
<tr>
<td>Alert Type</td>
<td>Type of alert</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Send an email alert to a specific user/group</td>
</tr>
<tr>
<td></td>
<td>*MSG - Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td></td>
<td>*CMD - Execute a command</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Send a notification to the system archive</td>
</tr>
<tr>
<td></td>
<td>*EMAILDIST - Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td></td>
<td>*TGCENTRAL - Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Details</td>
<td>Recipient details</td>
</tr>
<tr>
<td>Message to Send</td>
<td>Text included in the notification sent to the designated recipient</td>
</tr>
<tr>
<td>Alert Criteria - #Events</td>
<td>Number of alert events required to trigger a notification</td>
</tr>
<tr>
<td></td>
<td>Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Freq field.</td>
</tr>
<tr>
<td>Alert Criteria - Freq</td>
<td>Frequency of alert events required to trigger a notification. This field works in conjunction with the #Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.</td>
</tr>
</tbody>
</table>

See also

Working with Journal Monitor Rules

Manage Journal Monitor Alerts
Display Journal Monitor Activity Log

Use this task to display the list of triggered notifications (alerts) produced from the journal monitor log. Journal monitor log alerts are the messages sent when the criteria established for a journal monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system that needs to take action).

To display the list of journal monitor notifications

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 4 (Journal Monitor Rules).
4) In the OPT column for the desired history log rule, enter 30 (Work with Activity). The Work with Activity - Realtime Journal QSYS/QAUDJRN interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Type</td>
<td>Type of alert:</td>
</tr>
<tr>
<td></td>
<td>*CMD - Command executed</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Email sent</td>
</tr>
<tr>
<td></td>
<td>*MSG - System (login) message queued</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Syslog communication initiated</td>
</tr>
<tr>
<td>Activity Status</td>
<td>Status of alert</td>
</tr>
<tr>
<td>Activity Date</td>
<td>Date on which the alert was triggered</td>
</tr>
<tr>
<td>Activity Time</td>
<td>Time at which the alert was triggered</td>
</tr>
<tr>
<td>Activity Details</td>
<td>Description of alert</td>
</tr>
</tbody>
</table>

See also

Working with Journal Monitor Rules

Working with Monitor Activity Logs
Manage Journal Monitor Rules

Use this task to do the following:

- Access the Work with Rules - Realtime Journal QSYS/QAUDJRN Interface
- Edit Journal Monitor Rule
- Edit Journal Monitor Alerts

Tip: To manage the journal monitors rules, access from the Work with Rules - Realtime Journal QSYS/QAUDJRN interface.

Access the Work with Rules - Realtime Journal QSYS/QAUDJRN Interface

To access the Working with Rules interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 4 (Journal Monitor Rules).

Edit Journal Monitor Rule

Use this task to edit a journal monitor rule.

To edit a Journal Monitor Rule

2) In the OPT column for the desired journal monitor rule, enter 2 (Edit). The Work with Rules - Realtime Journal QSYS/QAUDJRN interface is displayed.
3) Modify the following editable field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Enter one of the options:</td>
</tr>
<tr>
<td></td>
<td>Y - Send an alert to the SIEM for this type of journal entry</td>
</tr>
<tr>
<td></td>
<td>N - Do not send an alert to the SIEM</td>
</tr>
<tr>
<td></td>
<td>Note: To see the SIEM log format in which the system sends alerts, refer to Manage Defaults.</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the desired calendar.</td>
</tr>
</tbody>
</table>

Edit Journal Monitor Rule Criteria

See Manage Journal Monitor Rule Criteria

Edit Journal Monitor Alerts
See Manage Journal Monitor Alerts

See also

Working with Journal Monitor

Display Journal Monitor Rules
Manage Journal Monitor Rule Criteria

Use this task to do the following:

- Access the Work with Rule Criteria - Realtime Journal QSYS/QAUDJRN Interface
- Edit Field Filter

Tip: To manage the journal monitor rule criteria, access from the Work with Rules - Realtime Journal QSYS/QAUDJRN interface.

Access the Work with Rule Criteria - Realtime Journal QSYS/QAUDJRN Interface

To access the Work with Rules - Realtime Journal QSYS/QAUDJRN interface

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 4 (Journal Monitor Rules).


Edit Field Filter

Use this task to edit the field-level filtering criteria.

Note: Field filters allow you to apply additional granularity to your monitor rules and to further limit alert notifications.

To edit the field filter


2) In the OPT column for the desired journal monitor rule, enter 9 (Filter).

3) Press Enter. The Work with Filtering Fields interface is displayed.

4) Place your cursor in the first available (blank) Opt column field and press the F4 (Select Fields) function key on your keyboard. The list of field(s) from which you can apply a filter are displayed in a Selection dialog.

5) Enter 1 in the Sel column for the field(s) you want to use for filtering.

6) Press Enter. The fields you selected are displayed in the Work with Filtering Fields interface.

7) Enter the field-specific criteria you want to use for filtering.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press the F10 function key on your keyboard.

Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis "(" in the Nest Str column. Likewise, to end a nested condition, enter a closing parenthesis ")" in the Nest End column.

8) Press Enter.
See also

Working with Journal Monitor Rules

Display Journal Monitor Rule Criteria
Manage Journal Monitor Alerts

Use this task to do the following:

- Access Work with Rules - Realtime Journal QSYS/QAUDJRN.
- Add Alert
- Delete Alert
- Edit Alert

**Tip:** To manage the journal monitor alerts, access from the Work with Rules - Realtime Journal QSYS/QAUDJRN interface.

**Access Work with Rules - Realtime Journal QSYS/QAUDJRN.**

To access the Work with Rules - Realtime Journal QSYS/QAUDJRN interface

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 4 (Journal Monitor Rules).

**Add Alert**

Use this task to add a journal monitor alert.

**To add alert**

2) Press the F6 (Add) function key. The Add Alert - QSYS/QAUDJRN interface is displayed
3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Type</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Send an email alert to a specific user/group</td>
</tr>
<tr>
<td></td>
<td>*MSG - Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td></td>
<td>*CMD - Execute a command</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Send a notification to the system archive</td>
</tr>
<tr>
<td></td>
<td>*EMAILDIST - Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td></td>
<td>*TGCENTRAL - Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Sequence</td>
<td>Enter the sequence in which you want alerts sent</td>
</tr>
<tr>
<td>Note:</td>
<td>You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.</td>
</tr>
<tr>
<td>Number of Events</td>
<td>Enter the number of alert events required to trigger a notification.</td>
</tr>
<tr>
<td></td>
<td>Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Event Frequency field.</td>
</tr>
</tbody>
</table>
Event Frequency | Enter the frequency of alert events required to trigger a notification. This field works in conjunction with the **Number of Events** field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.

**Event** | Enter the frequency unit:
- **DAYS** - Days
- **HR** - Hours
- **MIN** - Minutes
- **SEC** - Second

Tip: Press **F1** (Help) to access field descriptions.

4) Press **Enter** twice.

Delete Alert

Use this task to delete a journal monitor alert.

To delete alert

1) Access the **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface.

2) In the **OPT** column for the desired rule criteria, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct alert.

5) Press **Enter** twice.

Edit Alert

Use this task to edit a journal monitor alert.

To edit alert

1) Access the **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface.

2) In the **OPT** column for the desired rule criteria, enter **2** (Change).

3) Press **Enter**.

4) Modify the parameters as necessary.

5) Press **Enter** twice.

See also

*Working with Journal Monitor*

*Display Journal Monitor Alerts*
Run Journal Monitor Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run Journal Monitor Activity Report
- Run Journal Monitor Alert Report
- Run Journal Monitor Rule Report
- Run Journal Monitor Rules for SIEM Change Report

Tip: Refer to the TGDetect Report Reference for a complete list of report definitions.

Note: To work with default setting reports, access from the TGDetect Reports interface.

Access the TGDetect Reports Interface

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TGDetect Reports interface is displayed.

Run Journal Monitor Activity Report

Use this report to display the list of journal monitor activities.

To run the Journal Monitor Rule Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 1 (Activity History Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 5 (Journal Monitor Activity).
5) Press Enter.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Journal Monitor Alert Report
Use this report to display the list of journal monitor alerts.

**To run the Journal Monitor Alert Report**

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 2 (Configuration Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 8 (Journal Monitor Alerts).

5) Press Enter.

6) Modify the run criteria as necessary.

   Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Journal Monitor Rule Report**

Use this report to display the list of journal monitor rules.

**To run the Journal Monitor Rule Report**

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 2 (Configuration Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 7 (Journal Monitor Rules).

5) Press Enter.

6) Modify the run criteria as necessary.

   Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

**Run Journal Monitor Rules Details Change Report**

Use this report to display the list of changes made to the journal monitor rules details (criteria).

Tip: Auditing must be enabled to run change reports. See Add Auditing Defaults for a list of reports available.

**To run Journal Monitor Change Report**
1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter 3 (Change Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter 8 (Journal Monitor Rules Details Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Journal Monitor Rules for SIEM Report**

See [Run SIEM Reports](#)

**Run Journal Monitor Rules for SIEM Change Report**

See [Run SIEM Reports](#)

**See also**

- [Working with Journal Monitor Rules](#)
- [Working with SIEM Monitor Rules](#)
- [Working with Monitor Reports](#)
Message Queue Monitor

This section describes working with Message Queue (MSGQ) Monitor.

This section includes the following topics:

- Working with the Message Queue Monitor
- Display Message Queue Rules
- Display Message Queue Rule Criteria
- Display Message Queue Alerts
- Display Message Queue Activity Log
- Manage Message Queue Rules
- Manage Message Queue Rule Criteria
- Manage Message Queue Alerts
- Run Message Queue Reports

See also

Monitors
Working with the Message Queue Monitor

Use the **Message Queue (MSGQ) Monitor** to do the following:

- Display Message Queue Rules
- Display Message Queue Rule Criteria
- Display Message Queue Alerts
- Display Message Queue Activity Log
- Manage Message Queue Rules
- Manage Message Queue Rule Criteria
- Manage Message Queue Alerts
- Run Message Queue Reports

**Note**: To work with the Message Queue Monitor, you must access the **Work with Monitors** interface.

To access the Work with Monitors interface

1) Access the TGDetect **Main** menu.

2) At the **Selection or command** prompt, enter 1 (Working with Monitors).

3) Press **Enter**. The **Work with Monitors** interface is displayed.

See also

**Message Queue Monitor**
Display Message Queue Rules

Use this task to do the following with message queue rules:

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of message queue rules.

To display the list of message queue rules

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 3 (Message Queue Rules).


<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique Identifier assigned to message queue rule</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Name of the calendar that defines when the rule is applicable</td>
</tr>
</tbody>
</table>
| Daily Count| Number of daily alerts triggered by rule 
**Note**: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered. |
| Monthly Count| Number of monthly alerts triggered by rule                                |
| Yearly Count | Number of yearly alerts triggered by rule                                 |

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list
1) Access the **Work with Rules - MSGQ** interface.

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

   ![](tip.png)

   **Tip**: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Filter List**

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

![](tip.png)

**Tip**: Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules - MSGQ** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

- Working with Message Queue Rules
- Manage Message Queue Rules
Display Message Queue Rule Criteria

Use this task to do the following with message queue rule criteria:

- Display List
- Sort List
- Filter List

Display List

Use this task to display the list of message queue rule criteria

To display the list of message queue rule criteria
1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 3 (Message Queue Rules).
4) In the OPT column for the desired message queue rule, enter 10 (Rule Criteria). The Work with Rule Criteria - MSGQ interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique ID assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Name assigned to the rule for which you are displaying criteria</td>
</tr>
<tr>
<td>Minimum Severity</td>
<td>The rule severity level that must be met to trigger a message (notification)</td>
</tr>
<tr>
<td>MSGID</td>
<td>Unique ID assigned to the message rule criteria</td>
</tr>
<tr>
<td>Message File</td>
<td>File in which the message rule resides</td>
</tr>
<tr>
<td>Message File Library</td>
<td>Library in which the message rule resides</td>
</tr>
<tr>
<td>Description</td>
<td>Description of rule</td>
</tr>
<tr>
<td>Message Omit or Select</td>
<td>Identifies whether the rule criteria is used for selecting or omitting:</td>
</tr>
<tr>
<td></td>
<td>S (Select) - Rule criteria used to identify messages to include (trigger alerts)</td>
</tr>
<tr>
<td></td>
<td>O (Omit) - Rule criteria used to identify messages to exclude (should not trigger alerts)</td>
</tr>
<tr>
<td>Message Reply</td>
<td>Reply sent to the recipient</td>
</tr>
</tbody>
</table>

Sort List

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

To sort the list
1) Access the Work with Rules - MSGQ interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Filter List**

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

- **Tip:** Use wildcard asterisk to help define your subset.
  - Add an asterisk before text (e.g., *report) to find list items that end with specific text.
  - Add an asterisk after text (e.g., report*) to find list items that start with specific text.
  - Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules - MSGQ** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**.

**Note:** The system filters the results based on the criteria you defined for the subset.

**See also**

- Working with Message Queue Rules
- Manage Message Queue Rule Criteria
Display Message Queue Alerts

Use this task to display the list of alerts available for use with the message queue monitor. Message queue alerts are the messages sent when the criteria established for a message queue monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an alert to a designated recipient (user, user group, or system that needs to take action).

To display list message queue alerts

1) Access the TGDetect Main menu.
2) At the Selection or command prompt, enter 3 (Message Queue Rules).
3) Press Enter. The Work with Rules interface is displayed.
4) In the OPT column for the desired history log rule, enter **20** (Alerts). The Work with Alert - QSYS/QHST interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt Seq</td>
<td>The sequence in which alerts are sent</td>
</tr>
<tr>
<td><strong>Note:</strong> You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.</td>
<td></td>
</tr>
<tr>
<td>Alert Type</td>
<td>Type of alert</td>
</tr>
<tr>
<td><em>EMAIL</em> - Send an email alert to a specific user/group</td>
<td></td>
</tr>
<tr>
<td><em>MSG</em> - Send a system message (message that appears when a user logs into the system)</td>
<td></td>
</tr>
<tr>
<td><em>CMD</em> - Execute a command</td>
<td></td>
</tr>
<tr>
<td><em>SYSLOG</em> - Send a notification to the system archive</td>
<td></td>
</tr>
<tr>
<td><em>EMAILDIST</em> - Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
<td></td>
</tr>
<tr>
<td><em>TGCENTRAL</em> - Send a notification to TGCentral</td>
<td></td>
</tr>
<tr>
<td>Alert Details</td>
<td>Recipient details</td>
</tr>
<tr>
<td>Message to Send</td>
<td>Text included in the notification sent to the designated recipient</td>
</tr>
<tr>
<td>Alert Criteria - #Events</td>
<td>Number of alert events required to trigger a notification</td>
</tr>
<tr>
<td><strong>Alternatively</strong>, enter <strong>ALL</strong> to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Freq field.</td>
<td></td>
</tr>
<tr>
<td>Alert Criteria - Freq</td>
<td>Frequency of alert events required to trigger a notification. This field works in conjunction with the #Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.</td>
</tr>
</tbody>
</table>

See also

Working with Message Queue

Manage Message Queue Alerts
Display Message Queue Activity Log

Use this task to display the list of triggered notifications (alerts) produced from the Message queue monitor. The message queue alerts are the messages sent when the criteria established for a message queue monitor rule is met. In other words, when the criteria established for a rule is met, the system sends an email alert to a designated recipient (user, user group, or system that needs to take action).

To display the message queue activity log

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 3 (Message Queue Rules).

3) Press Enter. The Work with Rules interface is displayed.

4) In the OPT column for the desired history log rule, enter 30 (Work with Activity). The Work with Activity - *ALL interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity Type</td>
<td>Type of alert: EMAIL- Email sent</td>
</tr>
<tr>
<td>Activity Status</td>
<td>Status of alert</td>
</tr>
<tr>
<td>Activity Date</td>
<td>Date on which the alert was triggered</td>
</tr>
<tr>
<td>Activity Time</td>
<td>Time at which the alert was triggered</td>
</tr>
<tr>
<td>Activity Details</td>
<td>Description of alert</td>
</tr>
<tr>
<td>Activity Details</td>
<td>Description of activity</td>
</tr>
</tbody>
</table>

See also

Working with Message Queue

Working with Monitor Activity Logs
Manage Message Queue Rules

Use this task to do the following:

- Access the Work with Rules - MSGQ Interface
- Add Message Queue Rule
- Delete Message Queue Rule
- Edit Message Queue Rule
- Edit Message Queue Rule Criteria
- Edit Message Queue Alerts

**Note:** To manage the message queue rules, access from the *Work with Rules - MSGQ* interface.

Access the Work with Rules - MSGQ Interface

**To access the Working with Rules - MSGQ interface**

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 3 (Message Queue Rules).

3) Press Enter. The *Work with Rules - MSGQ* interface is displayed.

Add Message Queue Rule

Use this task to add a message queue rule.

**To add a message queue rule**

1) Access the *Work with Rules - MSGQ* interface.

2) Press the F6 (Add) function key. The *Work with Rules - Add*.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Enter a unique identifier for the message queue rule</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Enter a name for the message queue rule</td>
</tr>
<tr>
<td>Calendar</td>
<td>Enter the name of the calendar that defines when the rule is applicable</td>
</tr>
<tr>
<td></td>
<td>Tip: Enter <em>NONE</em> if no calendar is applicable</td>
</tr>
</tbody>
</table>

**Tip:** Press F1 (Help) to access field descriptions.

4) Press Enter twice.

Delete Message Queue Rule
Use this task to delete a message queue rule.

**To delete a message queue rule**

1) Access the **Work with Rules - MSGQ** interface.
2) In the **OPT** column for the desired message queue rule, enter 4 (Delete).
3) Press **Enter**.
4) Review the record to ensure you are deleting the correct message queue rule.
5) Press **Enter** twice.

**Edit Message Queue Rule**

Use this task to edit a message queue rule.

**To edit a message queue rule**

1) Access the **Work with Rules - MSGQ** interface.
2) In the **OPT** column for the desired message queue rule, enter 2 (Change).
3) Press **Enter**.
4) Modify the parameters as necessary.
5) Press **Enter** twice.

**Edit Message Queue Rule Criteria**

See **Manage Message Queue Rule Criteria**.

**Edit Message Queue Alerts**

See **Manage Message Queue Alerts**.

**See also**

*Working with Message Queue Rules*

*Display Message Queue Rules*
Manage Message Queue Rule Criteria

Use this task to do the following:

- Access the Work with Rule Criteria interface
- Add Rule Criteria
- Delete Rule Criteria
- Edit Rule Criteria
- Compare Fields
- Add Reply
- Limit Notifications to Messages that Require a Reply
- Change Severity

**Note:** To manage the message queue rule criteria, access from the Work with Rule Criteria - MSGQ interface.

Access the Work with Rule Criteria interface

To access the Work with Rule Criteria - MSGQ Interface

1) Access the TGDetect **Main** menu.

2) At the **Selection or command** prompt, enter **3** (Message Queue Rules).

3) **Press Enter.** The **Work with Rules - *All** interface is displayed.

4) **In the OPT column for the desired message queue rule, enter **10** (Rule Criteria).** The Work with Rule Criteria interface is displayed.

Add Rule Criteria

Use this task to add message queue rule criteria.

To add rule criteria

1) Access the **Work with Rule Criteria** interface.

2) **Press the **F6** (Add) function key.** The **Work with Rule Criteria - Add** interface is displayed.

3) **Complete the following fields.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message ID</td>
<td>Enter a unique ID for the message rule</td>
</tr>
<tr>
<td>Message File</td>
<td>Enter the file in which the message rule resides</td>
</tr>
<tr>
<td>Message File Library</td>
<td>Enter the library in which the message rule resides</td>
</tr>
</tbody>
</table>
Message Omit or Select | Enter whether the rule is used for selecting or omitting:  
S (Select) - Rule criteria used to identify messages to include (trigger alerts)  
O (Omit) - Rule criteria used to identify messages to exclude (should not trigger alerts)

Message Reply | Identifies whether a reply exists. Some actions require a reply in order to execute a follow-up action.  
**Note:** This allows you to set up the required reply to ensure that the workflow is not hindered.

---

4) Press **Enter** twice.

**Delete Rule Criteria**

Use this task to delete a message queue rule criteria.

**To delete rule criteria**

1) Access the **Work with Rule Criteria** interface.  
2) In the **OPT** column for the desired rule criteria, enter **4** (Delete).  
3) Press **Enter**.  
4) Review the record to ensure you are deleting the correct rule criteria.  
5) Press **Enter** twice.

**Edit Rule Criteria**

Use this task to edit the message queue rule criteria

**To edit rule criteria**

1) Access the **Work with Rule Criteria** interface.  
2) In the **OPT** column for the desired rule criteria, enter **2** (Change).  
3) Press **Enter**.  
4) Modify the parameters as necessary.  
5) Press **Enter** twice.

**Compare Fields**

Use this task to add additional filtering criteria specific to field values.

**Note:** This feature allows you to apply additional granularity to your monitor rules and to further limit alert notifications.
To compare fields

1) Access the Work with Rule Criteria interface.

2) In the OPT column for the desired rule criteria, enter 10 (Field Compare).

3) Press Enter.

4) Place your cursor in the first available (blank) Opt column field and press the F4 (Select Fields) function key on your keyboard.

5) Enter 1 in the Sel column for the field(s) you want to use in your filter.

6) Press Enter.

7) Enter the field-specific criteria you want to use for filtering.

8) Press Enter.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press the F10 function key on your keyboard.

Note: You can use up to five levels of nesting. To begin a nested condition, enter an open parenthesis "(" in the Nest Str column. Likewise, to end a nested condition, enter a closing parenthesis ")" in the Nest End column.
Use this task to create replies. Some actions require a reply (an answer to a question) in order to proceed.

**Note:** This feature allows you to set up a required reply in anticipation of this type of request to ensure that the workflow is not hindered.

### To create replies

1. Access the **Work with Rule Criteria - MSGQ** interface.
2. In the **OPT** column for the desired rule criteria, enter **20** (Work with Reply).
3. Press **Enter**.
4. Enter the necessary reply (C G D F).

<table>
<thead>
<tr>
<th>Reply</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Cancel</td>
</tr>
<tr>
<td>G</td>
<td>Continue processing at *GETIN</td>
</tr>
<tr>
<td>D</td>
<td>Obtain RPG formatted dump</td>
</tr>
<tr>
<td>F</td>
<td>Obtain full formatted dump</td>
</tr>
</tbody>
</table>

5. Press **Enter**.

### Limit Notifications to Messages that Require a Reply

Use this task when you want to limit message notification to only messages in a message queue that require a reply (C G D F).

### To limit Notification to only messages that require a reply

1. Access the **Work with Rule Criteria** interface.
2. Press the **F9** (Monitor MSGs Need Reply Only) function key. The **Work with Rule Criteria - Monitor MSGs Need Reply Only** interface is displayed.

**Note:** This option only appears when the message criteria you are modifying requires a reply. If a reply is required, you will see a **Y** in the **Reply** column.

3. Modify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Messages Requiring Reply Only</td>
<td>Enter one of the following:</td>
</tr>
<tr>
<td>*NO - Send notifications for all messages in the queue</td>
<td>*YES - Send notifications for only messages that required a reply</td>
</tr>
</tbody>
</table>

**Tip:** To see the complete list of messages present in a message queue (those that required a reply and those that do not), use the command **DSPMSG**.

4. Press **Enter**.
Change Severity

Use this task when you want to limit message notification by severity level. By default, the severity minimum is set to zero (00), which includes all severity levels. For example, if you want to exclude 00 (informational) messages from the notifications you receive, then change the minimum severity level to 20 (Error).

Tip: The severity scale (00-99) is based on IBM limits. See the IBM Knowledge Base for documentation on severity levels.

To change the minimum severity

1) Access the **Work with Rule Criteria** interface.

2) Press the **F7** (Change Severity) function key. The **Work with Rule Criteria - Change Severity** interface is displayed.

3) Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Severity</td>
<td>Enter the minimum severity level required:</td>
</tr>
<tr>
<td></td>
<td>00 - Information.</td>
</tr>
<tr>
<td></td>
<td>20 - Error</td>
</tr>
<tr>
<td></td>
<td>30 - Severe error</td>
</tr>
<tr>
<td></td>
<td>40 - Abnormal end of procedure or function</td>
</tr>
<tr>
<td></td>
<td>50 - Abnormal end of job</td>
</tr>
<tr>
<td></td>
<td>60 - System status</td>
</tr>
<tr>
<td></td>
<td>70 - Device integrity</td>
</tr>
<tr>
<td></td>
<td>80 - System alert</td>
</tr>
<tr>
<td></td>
<td>90 - System integrity</td>
</tr>
<tr>
<td></td>
<td>99 - Action</td>
</tr>
</tbody>
</table>

4) Press **Enter**.

See also

- Working with Message Queue Rules
- Display Message Queue Rule Criteria
Manage Message Queue Alerts

Use this task to do the following:

- Access Work with Alert - MSGQ interface.
- Add Alert
- Delete Alert
- Edit Alert

**Note:** To manage the message queue alerts, access from the **Work with Alert - MSGQ** interface.

### Access Work with Alert - MSGQ interface.

**To access the Work with Alert - MSGQ interface**

1) Access the TGDetect **Main** menu.

2) At the **Selection or command** prompt, enter 3 (Message Queue Rules).

3) Press **Enter**. The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alert). The **Work with Alert - MSGQ** interface is displayed.

### Add Alert

Use this task to add a message queue alert.

**To add alert**

1) Access the **Work with Alert - MSGQ** interface.

2) Press the **F6** (Add) function key. The **Add Alert - MSGQ** interface is displayed

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Type</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td>*EMAIL - Send an email alert to a specific user/group</td>
</tr>
<tr>
<td></td>
<td>*MSG - Send a system message (message that appears when a user logs into the system)</td>
</tr>
<tr>
<td></td>
<td>*CMD - Execute a command</td>
</tr>
<tr>
<td></td>
<td>*SYSLOG - Send a notification to the system archive</td>
</tr>
<tr>
<td></td>
<td>*EMAILDIST - Send an email alert to a specific user (legacy IBM method of sending email alerts)</td>
</tr>
<tr>
<td></td>
<td>*TGCENTRAL - Send a notification to TGCentral</td>
</tr>
<tr>
<td>Alert Sequence</td>
<td>Enter the sequence in which you want alerts sent</td>
</tr>
</tbody>
</table>

**Note:** You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.
Alert Message
Enter the text you want included in the notification sent to the designated recipient.

Number of Events
Enter the number of alert events required to trigger a notification. Alternatively, enter *ALL to trigger a notification every time an alert event occurs. For example, you might not want to receive a notification every time a user incorrectly enters a password at login, but you might want to receive a notification if a user completes 10 failed login attempts. This field works in conjunction with the Event Frequency field.

Event Frequency
Enter the frequency of alert events required to trigger a notification. This field works in conjunction with the Number of Events field. In the example provided above, you might want to send a notification only if the 10 failed login attempts occurred within a 1-hour period.

Event
Enter the frequency unit:
- DAYS - Days
- HR - Hours
- MIN - Minutes
- SEC - Second

Tip: Press F1 (Help) to access field descriptions.

4) Press Enter twice.

Delete Alert

Use this task to delete a message queue alert.

To delete alert
1) Access the Work with Alert - MSGQ interface.
2) In the OPT column for the desired rule criteria, enter 4 (Delete).
3) Press Enter.
4) Review the record to ensure you are deleting the correct alert.
5) Press Enter twice.

Edit Alert

Use this task to edit a message queue alert.

To edit alert
1) Access the Work with Alert - MSGQ interface.
2) In the OPT column for the desired rule criteria, enter 2 (Change).
3) Press Enter.
4) Modify the parameters as necessary.
5) Press Enter twice.
See also

Working with Message Queue

Display Message Queue Alerts
Run Message Queue Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run Message Queue Activity Report
- Run Message Queue Alert Report
- Run Message Queue Alert Change Report
- Run Message Queue Rule Report
- Run Message Queue Rules Header Changes Report
- Run Message Queue Rules Details Changes Report

Tip: Refer to the TGDetect Report Reference for a complete list of report definitions.

Note: To work with default setting reports, access from the TGDetect Reports interface.

Access the TGDetect Reports Interface

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.
2) At the Selection or command prompt, enter 20 (Reporting).
3) Press Enter. The TGDetect Reports interface is displayed.

Run Message Queue Activity Report

Use this report to display the list of message queue activities.

To run the Message Queue Activity Report

1) Access the TGDetect Reports interface.
2) At the Selection or command prompt, enter 1 (Activity History Reports).
3) Press Enter.
4) At the Selection or command prompt, enter 3 (Message Queue Activity).
5) Press Enter.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.
Run Message Queue Alert Report

Use this report to display the list of message queue alerts.

To run the Message Queue Alert Report

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 2 (Configuration Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 6 (Message Queue and Command Alerts).

5) Press Enter.

6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Message Queue Alert Change Report

Use this report to display the list of changes made to the message queue monitor alerts configuration.

Tip: Auditing must be enabled to run change reports. See Add Auditing Defaults for a list of reports available.

To run Message Queue Alert Change Report

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 3 (Change Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 5 (Msg Queue and Command Alerts Changes).

5) Press Enter.

6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Message Queue Rule Report

Use this report to display the list of message queue rules.
To run the Message Queue Rule Report

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 2 (Configuration Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 4 (Message Queue Rules).

5) Press Enter.

6) Modify the run criteria as necessary.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Message Queue Rules Header Changes Report

Use this report to display the list of changes made to message queue header (i.e., omit, select, reply, etc.).

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

To run Message Queue Rule Change Report

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 3 (Change Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 3 (Msg Queue Rules Header Changes).

5) Press Enter.

6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press F1 (Help) to access a field description. Press F4 (Prompt) for a list of valid field options.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

Run Message Queue Rules Details Changes Report

Use this report to display the list of changes made to message queue details (i.e., compare rule, filter sequence, etc.).

Tip: Auditing must be enabled to run change reports. See Add Auditing Defaults for a list of reports available.
To run Message Queue Rule Change Report

1) Access the TGDetect Reports interface.

2) At the Selection or command prompt, enter 3 (Change Reports).

3) Press Enter.

4) At the Selection or command prompt, enter 4 (Msg Queue Rules Details Changes).

5) Press Enter.

6) Modify the run criteria as necessary.

7) Press Enter. The status of the report is displayed at the bottom of the screen.

See also

Working with Message Queue Rules

Working with Monitor Reports
SIEM Monitor

This section describes working with the SIEM (Security Information and Event Management) Monitor. SIEMs help security teams analyze, detect, and prioritize threats.

This section includes the following topics:

- Working with SIEM Monitor
- Display SIEM Monitor Rules
- Display SIEM Monitor Rule Criteria
- Manage SIEM Monitor Rules
- Manage SIEM Monitor Rule Criteria
- Run SIEM Reports

See also

Monitors
Working with SIEM Monitor

Use the **SIEM (Security Information and Event Management) Monitor** to do the following:

- Display SIEM Monitor Rules
- Display SIEM Monitor Rule Criteria
- Manage SIEM Monitor Rules
- Manage SIEM Monitor Rule Criteria
- Run SIEM Reports

**Note**: To work with the SIEM Monitor, you must access the **Work with Monitors** interface.

**To access the Work with Monitors interface**

1) Access the TGDetect **Main** menu.

2) At the **Selection or command** prompt, enter 1 (Working with Monitors).

3) Press **Enter**. The **Work with Monitors** interface is displayed.

**See also**

SIEM Monitor
**Display SIEM Monitor Rules**

Use this task to do the following with SIEM (Security Information and Event Management) monitor rules:

**Display List**

Use this task to display the list of SIEM monitor rules.

**To display the list of SIEM monitor rules**

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter 6 (SIEM Monitor Rules).

3) Press **Enter**. The **Work with Rules - SIEM** interface is displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Identifies whether an alert is sent: &lt;br&gt;Y - Send an alert &lt;br&gt;N - Do not send an alert &lt;br&gt;<strong>Note</strong>: To see the SIEM log format in which the system sends alerts, refer to <strong>TGDetect Defaults</strong></td>
</tr>
<tr>
<td>Code</td>
<td>Identifies the type of audit trail journal &lt;br&gt;The following journal types are currently supported: &lt;br&gt;T - Security journal &lt;br&gt;U - User-defined journal</td>
</tr>
<tr>
<td>Type</td>
<td>Identifies the type of journal entry <strong>Note</strong>: Refer to the IBM Knowledge Center for a complete list of journal entry types and descriptions.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of journal entry</td>
</tr>
<tr>
<td>Field Filter</td>
<td>Identifies whether a field-level filter exists <strong>Note</strong>: Field-level filters all you to apply additional granularity to your monitor rules. &lt;br&gt;Y - Field-level filter exists &lt;br&gt;N - No field-level filter exists &lt;br&gt;<strong>Note</strong>: To see the filter definition, refer to <strong>Manage SIEM Monitor Rule Criteria</strong>.</td>
</tr>
<tr>
<td>Field Select</td>
<td>Identifies whether the data from all fields or a subset of fields is sent  &lt;br&gt;<strong>Note</strong>: Not all the data (fields) in a journal entry are relevant for security monitoring purposes; therefore, it might be helpful to limit which fields are sent. &lt;br&gt;Y - Send all fields &lt;br&gt;N - Send a subset of fields &lt;br&gt;<strong>Note</strong>: To see the subset of fields, refer to <strong>Manage SIEM Monitor Rule Criteria</strong>.</td>
</tr>
<tr>
<td>Daily Count</td>
<td>Number of daily alerts triggered by rule  &lt;br&gt;<strong>Note</strong>: The count is reset each time a new alert is triggered. In other words, if three alerts were triggered on a Monday, and you displayed this interface at the end of the day on Monday, this field would display the number 3. If no alerts were triggered on Tuesday, and you accessed this interface at the end of day on Tuesday, the value would still display the number 3 because no new alerts were triggered. If a single alert were triggered on Wednesday, and you accessed this interface at end of day on Wednesday, the value would then display the number 1. The value 1 would display in this field until a new alert is triggered.</td>
</tr>
<tr>
<td>Monthly Count</td>
<td>Number of monthly alerts triggered by rule</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Yearly Count</td>
<td>Number of yearly alerts triggered by rule</td>
</tr>
</tbody>
</table>

**Sort List**

Use this task to sort the list. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the Calendar column so that column heading initially appears in white text.

**To sort the list**

1) Access the **Work with Rules - SIEM** interface.

2) Place your cursor on the desired column heading.

3) Press the **F10** (Sort) function key.

Tip: The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Filter List**

Use this task to limit the calendars displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

- Add an asterisk before text (e.g., *report) to find list items that end with specific text.
- Add an asterisk after text (e.g., report*) to find list items that start with specific text.
- Add asterisks before and after to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with Rules - SIEM** interface.

2) Press the **F8** (Subset) function key.

3) Enter the criteria you want to use to define the subset.

4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.
Display SIEM Monitor Rule Criteria

Use this task to do the following with SIEM (Security Information and Event Management) monitor rule criteria:

- Display Field List
- Display Field Filters

Display Field List

Use this task to display the subset of fields communicated (sent) to the SIEM for analysis.

To display the list of selected fields

1) Access the TGDetect main menu.
2) At the Selection or command prompt, enter 6 (SIEM Monitor Rules).
4) Check the Field Select column.
   -- If Y appears in the column, then the system sends a subset of fields to the SIEM
   -- If N appears in the column, then the system sends all fields to the SIEM
5) In the Opt column for a journal entry type with a Y defined in the Field Select column, enter 8 (Field List). The Work with Field Selection interface is displayed.

Tip: If you enter 8 (Field List) in the Opt column for a journal entry type with N defined, no selected fields appear. See Manage SIEM Monitor Rule Criteria for instructions on adding select fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seq</td>
<td>Sequence in which fields are sent to the SIEM</td>
</tr>
<tr>
<td>Field Name</td>
<td>Name of field</td>
</tr>
<tr>
<td>Field Description</td>
<td>Description of field</td>
</tr>
</tbody>
</table>

Display Field Filters

Use this task to display field-level filtering criteria.

Note: Field filters allow you to apply additional granularity to your monitor rules and to further limit alert notifications.

To display the list of fields filters

1) Access the TGDetect main menu.
2) At the Selection or command prompt, enter 6 (SIEM Monitor Rules).
4) Check the **Field Filter** column.
   
   -- If **Y** appears in the column, then a field filter exists for the journal entry type
   
   -- If **N** appears in the column, then a field filter does not exist for the journal entry type

5) In the **Opt** column for a journal entry with a **Y** present in the **Field Filter** column, enter 9 (Filter). The **Work with Filtering Fields** interface is displayed.

   ![Tip: If you enter 9 (Filter) in the Opt column for a journal entry type with N defined, no filters appear. See Manage SIEM Monitor Rule Criteria for instructions on adding field filters.]

See also

- Working with SIEM Monitor Rules
- Manage SIEM Monitor Rule Criteria
Manage SIEM Monitor Rules

Use this task to do the following:

- Access the Work with Rules - SIEM Journal Interface
- Edit SIEM Monitor Rule
- Edit SIEM Monitor Rule Criteria

**Note:** To manage the SIEM (Security Information and Event Management) monitor rules, access from the Work with Rules - SIEM Journal interface.

Access the Work with Rules - SIEM Journal Interface

To access the Working with Rules - SIEM Journal interface

1) Access the TGDetect Main menu.

2) At the Selection or command prompt, enter 6 (SIEM Monitor Rules).


Edit SIEM Monitor Rule

Use this task to edit an SIEM monitor rule. **Note:** You can modify only the alert status using this task. See Manage SIEM Monitor Rule Criteria for additional instructions.

To edit an SIEM Monitor Rule


2) In the OPT column for the desired SIEM monitor rule, enter 2 (Edit). The Work with Rules - SIEM Journal - Edit Record interface is displayed.

3) Modify the following editable field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>Enter one of the options:</td>
</tr>
<tr>
<td></td>
<td>Y - Send an alert to the SIEM for this type of journal entry</td>
</tr>
<tr>
<td></td>
<td>N - Do not send an alert to the SIEM</td>
</tr>
</tbody>
</table>

**Note:** To see the SIEM log format in which the system sends alerts, refer to Manage Defaults.

Edit SIEM Monitor Rule Criteria

See Manage SIEM Monitor Rule Criteria.

See also

Working with SIEM Monitor Rules
Display SIEM Monitor Rules

Manage Defaults
Manage SIEM Monitor Rule Criteria

Use this task to do the following:

- **Access Work with Field Selection Interface**
- **Edit Field List**
- **Edit Field Filter**

**Note:** To manage SIEM (Security Information and Event Management) monitor rule criteria, access from the Work with Field Selection interface.

### Access Work with Field Selection Interface

To access the Work with Field Selection interface

1) Access the TGDetect **Main** menu.
2) At the **Selection or command** prompt, enter 6 (SIEM monitor Rules).
3) Press **Enter**. The **Work with Rules - SIEM Journal** interface is displayed.

### Edit Field List

Use this task to edit the subset of fields communicated (sent) to the SIEM for analysis.

To edit the field list

1) Access the **Work with Rules - SIEM Journal** interface.
2) In the **OPT** column for the desired SIEM monitor rule, enter 8 (Field List).
3) Press **Enter**. The **Work with Field Selection** interface is displayed.
4) Place your cursor in the first available (blank) **Opt** column field and press the **F4** (Select Fields) function key on your keyboard.

**Note:** The list of field(s) from which you can select are displayed in a **Selection** dialog.

5) Enter 1 in the **Sel** column for the field(s) you want to select (send).
6) Press **Enter**. The fields you selected are displayed in the **Work with Field Selection** interface.

**Tip:** You can reorder the sequence of fields by modifying the value in the **Seq** field.

7) Press **Enter**.

### Edit Field Filter

Use this task to edit the field-level filtering criteria.
To edit the field filter

2) In the OPT column for the desired SIEM monitor rule, enter 9 (Filter).
3) Press Enter. The Work with Filtering Fields interface is displayed.
4) Place your cursor in the first available (blank) Opt column field and press the F4 (Select Fields) function key on your keyboard. The list of field(s) from which you can apply a filter are displayed in a Selection dialog.
5) Enter 1 in the Sel column for the field(s) you want to use for filtering.
6) Press Enter. The fields you selected are displayed in the Work with Filtering Fields interface.
7) Enter the field-specific criteria you want to use for filtering.

Tips: An SQL-like format is used to create report filters. For a list of supported operators, press the F10 function key on your keyboard.

8) Press Enter.

See also

Working with SIEM Monitor Rules
Manage SIEM Monitor Rules
Run SIEM Reports

Use this task to generate the following SEIM (Security Information and Event Management) reports:

- **Access the TGDetect Reports Interface**
- **Run SIEM Activity Report**
- **Run SIEM Provider Report**
- **Run SIEM Provider Change Report**
- **Run Journal Monitor Rules for SIEM Report**
- **Run Journal Monitor Rules for SIEM Change Report**

**Tip:** Refer to the TGDetect Report Reference for a complete list of report definitions.

**Note:** To work with default setting reports, access from the TGDetect Reports interface.

**Access the TGDetect Reports Interface**

To access the TGDetect Reports interface

1) Access the TGSecure Main menu.

2) At the **Selection or command** prompt, enter **20** (Reporting).

3) Press **Enter**. The TGDetect Reports interface is displayed.

**Run SIEM Activity Report**

Use this report to display the list of command monitor activities.

**To run the SIEM Activity Report**

1) Access the TGDetect Reports interface.

2) At the **Selection or command** prompt, enter **1** (Activity History Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **6** (SIEM Activity).

5) Press **Enter**.

6) Modify the run criteria as necessary.

**Tip:** Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run SIEM Provider Report**
Use this report to display the SIEM providers.

**To run the SIEM Provider Report**
1) Access the TGDetect Reports interface.
2) At the **Selection or command** prompt, enter **2** (Configuration Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **3** (SIEM Providers).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run SIEM Provider Change Report**

Use this report to display the list of changes made to SIEM providers.

Tip: Auditing must be enabled to run change reports. See Add Auditing Defaults for a list of reports available.

**To run SIEM Provider Change Report**
1) Access the TGDetect Reports interface.
2) At the **Selection or command** prompt, enter **3** (Change Reports).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **2** (SIEM Providers Changes).
5) Press **Enter**.
6) Modify the run criteria as necessary.

Tip: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Journal Monitor Rules for SIEM Report**

Use this report to display the list of journal monitor rules for SIEM.

**To run the Journal Monitor Rules for SIEM Report**
1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter **2** (Configuration Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **9** (Journal Monitor Rules for SIEM).

5) Press **Enter**.

6) Modify the run criteria as necessary.

   - **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**Run Journal Monitor Rules for SIEM Change Report**

Use this report to display the changes made to the journal monitor rules for SIEM.

   - **Tip**: Auditing must be enabled to run change reports. See **Add Auditing Defaults** for a list of reports available.

**To run SIEM Provider Change Report**

1) Access the **TGDetect Reports** interface.

2) At the **Selection or command** prompt, enter **3** (Change Reports).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **7** (Journal Monitor Rules for SIEM Changes).

5) Press **Enter**.

6) Modify the run criteria as necessary.

   - **Tip**: Place your cursor in a field and press **F1** (Help) to access a field description. Press **F4** (Prompt) for a list of valid field options.

7) Press **Enter**. The status of the report is displayed at the bottom of the screen.

**See also**

- Working with SIEM Monitor Rules
- Working with Journal Monitor Rules
- Working with Monitor Reports
Rules

This section includes the following topic:

- Working with Monitor Rules

Command Monitor Rules

- Display Command Monitor Rules
- Display Command Monitor Rule Criteria
- Manage Command Monitor Rules
- Manage Command Monitor Rule Criteria

History Log Monitor Rules

- Display History Log Rules
- Display History Log Rule Criteria
- Manage History Log Rules
- Manage History Log Rule Criteria

Journal Monitor Rules

- Display Journal Monitor Rules
- Display Journal Monitor Rule Criteria
- Manage Journal Monitor Rules
- Manage Journal Monitor Rule Criteria

Message Queue Monitor Rules

- Display Message Queue Rules
- Display Message Queue Rule Criteria
- Manage Message Queue Rules
- Manage Message Queue Rule Criteria

Message SIEM Monitor Rules

- Display SIEM Monitor Rules
- Display SIEM Monitor Rule Criteria
- Manage SIEM Monitor Rules
- Manage SIEM Monitor Rule Criteria

See also

Getting Started
Working with Monitor Rules

This section describes working with monitor rules.

**Note:** Each monitor type has its own associated rule format.

**Command Monitor Rules**

- Display Command Monitor Rules
- Display Command Monitor Rule Criteria
- Manage Command Monitor Rules
- Manage Command Monitor Rule Criteria

**History Log Monitor Rules**

- Display History Log Rules
- Display History Log Rule Criteria
- Manage History Log Rules
- Manage History Log Rule Criteria

**Journal Monitor Rules**

- Display Journal Monitor Rules
- Display Journal Monitor Rule Criteria
- Manage Journal Monitor Rules
- Manage Journal Monitor Rule Criteria

**Message Queue Monitor Rules**

- Display Message Queue Rules
- Display Message Queue Rule Criteria
- Manage Message Queue Rules
- Manage Message Queue Rule Criteria

**Message SIEM Monitor Rules**

- Display SIEM Monitor Rules
- Display SIEM Monitor Rule Criteria
- Manage SIEM Monitor Rules
- Manage SIEM Monitor Rule Criteria

**Note:** To work with rules, you must access the Work with Rules interface.

To access the Work with Rules interface

Trinity Guard 124
1) Log into TGDetect. The **Main** menu appears.

2) At the **Selection or command** prompt, enter 1 (Working with Monitors).

3) Press **Enter**. The **Work with Monitor** interface is displayed.

4) In the **Opt** column, enter **10** (Work with Rules).

5) Press **Enter**. The **Work with Rules** interface is displayed.

**See also**

- Log into TGDetect
- Working with Monitors
- Working with Monitor Reports
Activity Log

This section includes the following topic:

- Working with Monitor Activity Log

See also

Getting Started
Working with Monitor Activity Log

This section describes working with monitor activity logs.

ℹ️ **Note:** Each monitor type (except the SIEM monitor) produced an activity log

- Display Command Monitor Activity Log
- Display History Log Activity Log
- Display Journal Monitor Activity Log
- Display Message Queue Activity Log

**See also**

- Log into TGDetect
- Working with Monitors
- Working with Monitor Rules
Reports

This section includes the following topic:

- Working with Monitor Reports

See also

Getting Started
Working with Monitor Reports

This section describes working with monitor reports.

**Note:** In order to work with the monitor reports, you must access the TGDetect Reports interface.

To access the TGDetect Reports interface

1) Log into TGDetect. The Main menu appears.

2) At the Selection or command prompt, enter 20 (Reporting).

3) Press Enter. The TGDetect Reports interface is displayed.

Each monitor type has its own associated report.

- Run Command Monitor Reports
- Run Default Reports
- Run History Log Reports
- Run Journal Monitor Reports
- Run Message Queue Reports
- Run Monitor Master Reports
- Run SIEM Reports

**Tip:** Auditing must be enabled to run change reports. See Add Auditing Defaults for additional information.

See also

- Log into TG Detect
- Working with Monitors
- Working with Monitor Rules
- Manage Defaults
Groups

This section includes the following topic:

- Working with User Groups

See also

Getting Started
User Groups

This section describes how to work with Users and User Groups.

This section includes the following topics:

- Working with User Groups
- Display List of User Groups
- Display List of Users in a Group
- Manage User Groups
- Manage Users in a Group
- Run User Groups Report

See also

Groups
Working with User Groups

This section describes how to work with User Groups.

This section includes the following topics:

Note: To work with user groups, you must access the Work with User Groups interface.

Access the Work with User Groups Interface

To display the Work with User Groups interface

1) Access the Main menu.

2) At the Selection or command prompt, enter 10 (Work with User Groups).

3) Press Enter. The Work with User Groups interface is displayed.

See also

Groups
Display List of User Groups

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List
- Filter List

**Note:** To work with user groups, you must access the **Work with User Groups** interface.

**Display Lists of User Groups**

Use this task to display the list of user groups.

**To display the list of user groups**

1) Access the **Main** menu.

2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit | 1. At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the **11** (Work with User Groups). |
| TGDetect | At the **Selection or command** prompt, enter **10** (Work with User Groups). |
| TGEncrypt | 1. At the **Selection or command** prompt, enter **4** (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the **1** (Work with User Groups). |
| TGSecure | 1. At the **Selection or command** prompt, enter **31** (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the **1** (Work with User Groups). |

**Sort List**
Use this task to sort the list of available networks. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Group Name** column so that column heading initially appears in white text.

**To sort the list**

1) Access the **Work with User Groups** interface.
2) Place your cursor on the desired column heading.
3) Press the **F10** (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click **F10** again.

**Move to Position in List**

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

**To move to a specific position within the list**

1) Access the **Work with User Groups** interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the **Position to** field, and enter a letter, word, phrase, or number.
4) Press **Enter**.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

**Filter List**

Use this task to limit the user groups displayed in the list by defining a subset for filtering purposes.

**Tip:** Use wildcard asterisk to help define your subset.

– Add an asterisk before text (e.g., *report) to find list items that end with specific text.
– Add an asterisk after text (e.g., report*) to find list items that start with specific text.
– Add asterisks before and after text to find list items that contain specific text anywhere in the name.

**To filter the list using a subset**

1) Access the **Work with User Groups** interface.
2) Press the **F8** (Subset) function key.
3) Enter the criteria you want to use to define the subset.
4) Press **Enter**. The system filters the results based on the criteria you defined for the subset.

**See also**

*Working with User Groups*
Display List of Users in a Group

Use this task to do the following with user groups:

- Display Lists of User Groups
- Sort List
- Move to Position in List

Note: To work with user groups, you must access the Work with User Groups interface.

Display Lists of User Groups

Use this task to display the list of user groups.

To display the list of user groups

1) Access the Main menu.
2) Do one of the following:

Note: Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit  | 1. At the Selection or command prompt, enter the 3 (Job Activity Monitor).  
2. Press Enter.  
3. At the Selection or command prompt, enter the 11 (Work with User Groups). |
| TGDetect | At the Selection or command prompt, enter 10 (Work with User Groups). |
| TGEncrypt| 1. At the Selection or command prompt, enter 4 (Work with Groups).  
2. Press Enter.  
3. At the Selection or command prompt, enter the 1 (Work with User Groups). |
| TGSecure | 1. At the Selection or command prompt, enter 31 (Work with Groups).  
2. Press Enter.  
3. At the Selection or command prompt, enter the 1 (Work with User Groups). |

Sort List

Use this task to sort the list of available users.
To sort the list

1) Access the Work with Users interface.
2) Place your cursor on the desired column heading.
3) Press the F10 (Sort) function key.

**Tip:** The system sorts the list in ascending order based on the selected column heading. To reverse the sort (descending order), click F10 again.

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list and you want to avoid paging down.

To move to a specific position within the list

1) Access the Work with Users interface.
2) Sort the list based on the desired column heading.
3) Place your cursor in the Position to field, and enter a letter, word, phrase, or number.
4) Press Enter.

**Note:** The system jumps to the location within the sorted column where the letter, word, phrase, or number first appears.

See also

Working with User Groups
Manage User Groups

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Add User Group
- Edit User Group
- Copy User Group
- Delete User Group

**Note:** To manage user groups, access the **Work with User Groups** interface.

Access the Work with User Group Interface

**To access the Work with User Groups interface**

1) Access the **Main** menu.

2) Do one of the following:

**Note:** Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit   | 1. At the **Selection or command** prompt, enter the 3 (Job Activity Monitor).<br>2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 11 (Work with User Groups). |
| TGDetect  | At the **Selection or command** prompt, enter 10 (Work with User Groups). |
| TGEncrypt | 1. At the **Selection or command** prompt, enter 4 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |
| TGSecure  | 1. At the **Selection or command** prompt, enter 31 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |

Add User Group

Use this task to add a user group.
To add user group

1) Access the Work with User Groups interface.
2) Press the F6 (Add) function key.
3) Enter the name (ID) you want to assign to the group.

Tip: Group names must begin with a colon and cannot contain spaces.

4) Enter a description for the group.
5) Press Enter twice.

Edit User Group

Use this task to edit a user group.

To edit user group

1) Access the Work with User Groups interface.
2) In the OPT column for the desired group, enter 2 (Edit).
3) Press Enter.
4) Modify the description as necessary.

Note: You cannot edit the name.

5) Press Enter twice.

Copy User Group

Use this task to copy a user group.

To copy user group

1) Access the Work with User Groups interface.
2) In the OPT column for the desired group, enter 3 (Copy).
3) Press Enter.
4) Modify the description as necessary.
5) Press Enter twice.

Delete User Group

Use this task to delete a user group

To delete user group

1) Access the Work with User Groups interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct group.

5) Press **Enter** twice.

**See also**

Working with User Groups
Manage Users in a Group

Use this task to do the following with user groups:

- Access the Work with User Group Interface
- Edit a User
- Delete a User

**Note**: To manage users, access the Work with Users interface.

Access the Work with User Group Interface

To access the Work with User Groups interface

1) Access the **Main** menu.
2) Do one of the following:

**Note**: Groups are a common feature used in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
</table>
| TGAudit  | 1. At the **Selection or command** prompt, enter the 3 (Job Activity Monitor).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 11 (Work with User Groups). |
| TGDetect | At the **Selection or command** prompt, enter 10 (Work with User Groups). |
| TGEncrypt| 1. At the **Selection or command** prompt, enter 4 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |
| TGSecure | 1. At the **Selection or command** prompt, enter 31 (Work with Groups).  
2. Press **Enter**.  
3. At the **Selection or command prompt**, enter the 1 (Work with User Groups). |

Add a User

Use this task to add a user.

To add user
1) Access the **Work with Users** interface.

2) Press the **F6** (Add) function key.

3) Enter the name (ID) you want to assign to the user.

   **Tip:** Names cannot contain spaces.

4) Enter a description for the user.

5) Press **Enter** twice.

   **Note:** If the user already exists, you will see a *YES in the **Exists on Server** field the first time you press **Enter**. If the user does not exist, you will see *No in the **Exists on Server** field the first time you press **Enter**.

### Edit a User

Use this task to edit a user.

   **Note:** You can only edit the user description, not the user name.

#### To edit user

1) Access the **Work with Users** interface.

2) In the **OPT** column for the desired user, enter 2 (Edit).

3) Press **Enter**.

4) Modify the user description as necessary.

   **Note:** You cannot edit the user name.

5) Press **Enter** twice.

### Delete a User

Use this task to delete a user.

#### To delete user

1) Access the **Work with Users** interface.

2) In the **OPT** column for the desired user, enter 4 (Delete).

3) Press **Enter**.

4) Review the record to ensure you are deleting the correct user.

5) Press **Enter** twice.
See also

Working with User Groups
Network/Server Groups

This section describes how to work with Networks and Network Groups.

This section includes the following topics:

- Working with Network/Server Groups
- Display List of Network/Server Groups
- Display List of Networks in a Group
- Manage Network/Server Groups
- Manage Networks in a Group
- Run Network Groups Report

See also

Groups
Working with Network/Server Groups

Note: To work with network groups, you must access the **Work with Network/Server Groups** interface.

To access the Work with Network/Server Groups interface

1) Access the **Main** menu.

2) Do one of the following:

   Note: Network/server groups are a common feature in multiple TG products.

<table>
<thead>
<tr>
<th>Product</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGEncrypt</td>
<td>At the <strong>Selection or command</strong> prompt, enter 4 (Work with Groups).</td>
</tr>
<tr>
<td>TGSecure</td>
<td>At the <strong>Selection or command</strong> prompt, enter 31 (Work with Groups).</td>
</tr>
</tbody>
</table>

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **2** (Work with Network/Server Groups).

5) Press **Enter**. The **Work with Network Groups** Interface is displayed.

See also

*Network/Server Groups*
Email/Syslog Setup

This section includes the following topic:

- Working with Email/Syslog Setup

See also

Getting Started
Working with Email _Syslog Setup

This section describes working with email and/or Syslog setup options. These settings tell the system where and how to send alerts outside of the system.

- Email Setup
- Syslog Setup

**Note:** To work with notifications setup options, you must access the Email/Syslog Configuration interface.

To access the Email/Syslog Configuration interface

1) Log into to TGDetect. The **Main** menu appears.

2) At the **Selection or command** prompt, enter **12** (Email/Syslog Configuration).

3) Press **Enter**. The **Email/Syslog Configuration** interface is displayed.

**See also**

Log into TGDetect
Email Setup
Working with Email Alerts

This section describes working with email alerts.

Note: Each monitor (except the SIEM monitor) produces monitor specific alerts.

Command Monitor Alerts

- Display Command Monitor Alerts
- Manage Command Monitor Alerts

History Log Monitor Alerts

- Display History Log Alerts
- Manage History Log Alerts

Journal Monitor Alerts

- Display Journal Monitor Alerts
- Manage Journal Monitor Alerts

Message Queue Monitor Alerts

- Display Message Queue Alerts
- Manage Message Queue Alerts

See also

Log into TGDetect

Working with Monitors

Working with Monitor Rules
Working with Email Setup

This section describes tasks you need to perform to set up email (SMTP) alerts.

- Manage email setup

**Note:** To work with email setup, you must access the **Email Setup** interface.

To access the Email Setup interface

1) Log into TGDetect. The **Main** menu appears.

2) At the **Selection or command** prompt, enter **12** (Email/Syslog Configuration).

3) Press **Enter**. The **Email/Syslog Configuration** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Email Setup - SMTP). The **Email Setup** interface is displayed.

See also

- Log into TGDetect
- Working with Email/Syslog Setup
Manage Email Setup

Use this task to do the following:

**Note:** The tasks must be completed in the following order.

1) Add SMTP host table entry
2) Add SMTP directory entry
3) Change TCP/IP domain
4) Change mail distribution attributes
5) Change SMTP attributes
6) Change SMTPA via IBM i Navigator
7) Restart QSNADS, MSF and SMTP
8) Add SMTP user

**Note:** To manage email setup, access from the **Email Setup** interface.

Access the Email Setup Interface

To access the Email Setup interface

1) Log into TGDetect. The Main menu appears.
2) At the Selection or command prompt, enter **12** (Email/Syslog Configuration).
3) Press Enter. The **Email/Syslog Configuration** interface is displayed.
4) At the Selection or command prompt, enter **1** (Email Setup - SMTP). The **Email Setup** interface is displayed.

(1) Add SMTP Host Table Entry

Use this task to add the SMTP host information.

To add SMTP host table

1) Access the **Email Setup** interface.
2) At the Selection or command prompt, enter **1** (Add SMTP Host Table Entry). The **Add TCP/IP Host Table Entry (ADDTCPHTE)** interface is displayed.
3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet address</td>
<td>Enter the IP address of the SMTP server</td>
</tr>
<tr>
<td>Host name</td>
<td>Enter the host (website) URL for the SMTP server</td>
</tr>
</tbody>
</table>
4) Press **Enter** twice.

**2) Add SMTP Directory Entry**

Use this task to add the SMTP directory.

**To add SMTP directory entry**

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter **2** (Add SMTP Directory Entry). The **Add Directory Entry (ADDDIRE)** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network user ID</td>
<td>Enter the user ID required to log into the network</td>
</tr>
<tr>
<td>Last name</td>
<td>Enter the user's last name</td>
</tr>
<tr>
<td>First name</td>
<td>Enter the user's first name</td>
</tr>
<tr>
<td>Middle name</td>
<td>Enter the user's middle name</td>
</tr>
<tr>
<td>Preferred name</td>
<td>Enter the user's preferred name</td>
</tr>
</tbody>
</table>

4) Press **Enter** twice.

**3) Change TCP/IP Domain**

Use this task to change the TCP/IP domain.

**To change TCP/IP domain**

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter **3** (Change TCP/IP Domain). The **Change TCP/IP Domain (CHGTCPDMN)** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Enter the name of the TCP/IP host</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter the web domain of the TCP/IP host</td>
</tr>
</tbody>
</table>
Internet address   Enter the IP address of the TCP/IP host

**Tip:** Press **F1** (Help) to access field descriptions.

4) Press **Enter** twice.

**4) Change Mail Distribution Attributes**

Use this task to mail distribution attributes.

**To change mail distribution attributes**

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter 4 (Change Mail Distribution Attributes). The **Change Mail Distribution Attributes (CHGDSTA)** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep recipients</td>
<td>Enter one of the following options: <em>ALL</em> - Keep all recipients</td>
</tr>
<tr>
<td></td>
<td><em>BCC</em> - Keep recipients who are blind copied</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Same as previous</td>
</tr>
<tr>
<td></td>
<td><em>NONE</em> - Do not keep recipients</td>
</tr>
<tr>
<td>Use MSF for local</td>
<td>Enter one of the following options: <em>YES</em> - Enable MSF (Message Switching</td>
</tr>
<tr>
<td></td>
<td>Facility)</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Disable MSF</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Same as previous</td>
</tr>
<tr>
<td>User ID</td>
<td>User ID of sender</td>
</tr>
<tr>
<td>Address</td>
<td>Email address of sender</td>
</tr>
</tbody>
</table>

**Tip:** Press **F1** (Help) to access field descriptions.

4) Press **Enter** twice.

**5) Change SMTP Attributes**

Use this task to change the SMTP attributes.

**To change SMTP attributes**

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter 5 (Change SMTP Attributes). The **Change SMTP Attributes (CHGSMTPA)** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

**Tip:** Press **F1** (Help) to access field descriptions.
<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autostart server</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Enable autostart</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Disable autostart</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Clear e-mail on start-up</td>
<td>Enter one of the following options</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Enable clear e-mail on start-up</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Disable clear e-mail on start-up</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>E-mail directory type</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>SMTP</em> - Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td></td>
<td><em>SMTPMSF</em> - Simple Mail Transfer Protocol (with Message Switching Facility)</td>
</tr>
<tr>
<td></td>
<td><em>SDD</em> - System Distribution Directory</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by minute: Number of retries</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of access retries per minute. The max number of retries is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by minute: Time interval</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of minutes to wait between retries. The max number of minutes is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by day: Number of retries</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of access retries per day. The max number of retries is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by day: Time interval</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of days to wait between retries. The max number of days is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by hour: Number of retries</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of access retries per hour. The max number of retries is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Retries by hour: Time interval</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>0-99</em> - Enter the number of hours to wait between retries. The max number of hours is 99.</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Coded character set identifier</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>1-65533</em> - Enter the ASCII coded character set identifier (CCSI) used to map all single-byte</td>
</tr>
<tr>
<td></td>
<td>character sets (SBCS) data on outgoing mail</td>
</tr>
<tr>
<td></td>
<td><em>DFT</em> - Use system default value</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use the value previously set (no change)</td>
</tr>
<tr>
<td>Support ETRN for server</td>
<td>Enter one of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>YES</em> - Enable support for ETRN (Extended Turn) servers</td>
</tr>
<tr>
<td></td>
<td><em>NO</em> - Disable support for ETRN</td>
</tr>
<tr>
<td></td>
<td><em>SAME</em> - Use system default value</td>
</tr>
</tbody>
</table>

**Tip:** Press F1 (Help) to access field descriptions.
4) Press Enter twice.

(6) Change SMTPA via IBM i Navigator

Use this task to change the SMTP via the IBM i Navigator feature.

- **Note:** The step is identified in the menu, but it is not completed within TGDetect. The menu item is a placeholder meant to remind you to complete the step, and it should not be used to complete the step.

To change the SMTPA via the IBM i Navigator

1) Click the Windows Start menu.
2) Select IBM i Access for Windows option.

- **Tip:** You might need to scroll down to find the program.

3) Select System i Navigator.
4) Expand the desired server (agent) under My Connections.
5) Expand Network.
6) Expand Servers.
7) Select TCP/IP.

- **Note:** The list of installed servers appears in the right pane.

8) In the right pane, scroll down until you see SMTP.
9) Right-click on SMTP and select Properties. The SMTP Properties dialog box is displayed.
10) Select the Authentication tab.
11) In the Logon information for relay server area, you can see the list of existing SMTP servers.
12) Click the Add button. The Add Host Logon Information dialog box is displayed.
13) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Enter the name of your mail server (e.g., SMTP.TrinityGuard.com)</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name</td>
</tr>
<tr>
<td>User password</td>
<td>Enter the user's password</td>
</tr>
<tr>
<td>Confirm user password</td>
<td>Enter the user's password again for verification</td>
</tr>
</tbody>
</table>

4) Press OK.
(7) Restart QSNADS, MSF and SMTP

Use this task to restart QSNADS.

To restart QSNADS, MSF and SMTP

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter 7 (Restart QSNADS, MSF and SMTP)

   **Note:** An "X" appears in the bottom of the screen indicating that the task is in process. When the "X" disappears, which indicates that the task is complete, move on to the next step.

(8) Add SMTP User

Use this task to add the SMTP user(s).

To add SMTP user

1) Access the **Email Setup** interface.

2) At the **Selection or command** prompt, enter 8 (Add SMTP User). The **Add User SMTP (ADDDIRE)** interface is displayed.

3) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile</td>
<td>Enter the TG profile name of the user</td>
</tr>
<tr>
<td>SMTP mailbox alias</td>
<td>Enter the SMTP mailbox alias used to receive email notifications</td>
</tr>
<tr>
<td>Domain index</td>
<td>Enter the domain index. <strong>Note:</strong> A domain index determining which databases and/or files systems are to be included in the full text index.</td>
</tr>
</tbody>
</table>

**Tip:** Press **F1** (Help) to access field descriptions.

4) Press **Enter** twice.

See also

*Working with Email Setup*
Syslog Setup

This section includes the following topic:
Working with Syslog Setup

This section describes tasks you need to perform to setup Syslog alerts.

Manage Syslog setup

ℹ️ **Note:** To work with communication setup, you must access the **Syslog Provider** interface.

To access the Syslog Provider interface

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter **12** (Email/SNMP/Communication).

3) Press **Enter**. The **Email/Syslog Configuration** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Syslog Configuration).

5) Press **Enter**.

**Note:** The **Syslog Provider** interface is displayed.

See also

- Log into TGDetect
- Working with Email/Syslog Setup
Manage Syslog Setup

Use this task to do the following:

- Access the Email/Syslog Configuration Interface
- Display List of Syslog Providers
- Add Syslog Provider
- Edit Syslog Provider
- View Message Queue, History Log, and Command Rules
- View Journal Rules

**Note:** To manage the Syslog setup, access from the Email/Syslog Configuration interface.

Access the Email/Syslog Configuration Interface

Use this task to access the Email/Syslog Configuration interface.

**To access the Working with Rules - MSGQ interface**

1) Access the TGDetect main menu.

2) At the **Selection or command** prompt, enter 12 (Email/SNMP/Communication).

3) Press **Enter**. The Email/Syslog Configuration interface is displayed.

Display List of Syslog Providers

Use this task to display the list of Syslog (system log) providers. TGDetect comes with a number of built-in provider definitions that you can edit as necessary.

**To display the list of Syslog provider**

1) Access the **Email/Syslog Configuration** interface.

2) At the **Selection or command** prompt, enter 2 (Syslog Configuration).

3) Press **Enter**. The Syslog Provider interface is displayed.

4) Click the **Page Down** key on your keyboard to see the list of Syslog providers.

**Note:** Each provider presents on a separate page.

Add Syslog Provider

Use this task to add a Syslog provider.

**To add a Syslog providers**

1) Access the **Email/Syslog Configuration** interface.
2) At the **Selection or command** prompt, enter 2 (Syslog Configuration).

3) Press **Enter**. The **Syslog Provider** interface is displayed.

4) Press the **F10** (Entry) function key on your keyboard.

5) Complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Provider Name</td>
<td>Enter the name of the Syslog provider</td>
</tr>
<tr>
<td>Syslog Provider</td>
<td>Description</td>
</tr>
<tr>
<td></td>
<td>Enter a short description of the Syslog provider</td>
</tr>
<tr>
<td>Syslog IP Address</td>
<td>Enter the IP address at which the Syslog provider resides</td>
</tr>
<tr>
<td>Syslog Port</td>
<td>Enter the port you want to use to communicate to the Syslog provider</td>
</tr>
<tr>
<td>Syslog Protocol</td>
<td>Enter the protocol you want to use to communicate with the Syslog provider:</td>
</tr>
<tr>
<td></td>
<td>SSL - Secure socket layer protocol</td>
</tr>
<tr>
<td></td>
<td>TCP - Transmission control protocol</td>
</tr>
<tr>
<td></td>
<td>UDP - User datagram protocol</td>
</tr>
<tr>
<td>Message Log Format</td>
<td>Enter the message log format you want to use to communicate with the Syslog</td>
</tr>
<tr>
<td></td>
<td>provider:</td>
</tr>
<tr>
<td></td>
<td>CEF - Common Event Format</td>
</tr>
<tr>
<td></td>
<td>GELF - Graylog Extended Log Format</td>
</tr>
<tr>
<td></td>
<td>LEEF - Log Event Extended Format</td>
</tr>
<tr>
<td></td>
<td>SYSLOG - System Log</td>
</tr>
<tr>
<td>Syslog Facility</td>
<td>Enter the type of program logging the message</td>
</tr>
<tr>
<td>Syslog Severity</td>
<td>The severity of the message as defined by Syslog</td>
</tr>
</tbody>
</table>

**Tip:** Press **F1** (Help) to access field descriptions.

6) Press **Enter**.

**Edit Syslog Provider**

Use this task to edit an existing Syslog provider.

**To edit a Syslog provider**

1) Access the **Email/Syslog Configuration** interface.

2) At the **Selection or command** prompt, enter 2 (Syslog Configuration).

3) Press **Enter**. The **Syslog Provider** interface is displayed.

4) Press the **F10** (Entry) function key on your keyboard.

5) Modify the parameters as necessary.
6) Press Enter.

**View Message Queue, History Log, and Command Rules**

Use this task to view rules using the Syslog provider.

**To view Message Queue, History Log and Command Rules**

1) Access the **Email/Syslog Configuration** interface.

2) At the **Selection or command** prompt, enter 6 (MSGQ/QHST/CMD Rules).

3) Press Enter. All rules using the **Syslog Provider** are displayed.

**View Journal Rules**

Use this task to view journal rules using the Syslog provider.

**To view Message Queue, History Log and Command Rules**

1) Access the **Email/Syslog Configuration** interface.

2) At the **Selection or command** prompt, enter 7 (Journal Rules).

3) Press Enter. All journal rules using the **Syslog Provider** are displayed.

**See also**

*Working with Syslog Setup*
Appendices

- APPENDIX - TGDetect Revisions
  - Version 2.4 - TGDetect User Guide Revisions
  - Version 2.3 - TGDetect User Guide Revisions
  - Version 2.2 - TGDefect User Guide Revisions
  - Version 2.1 - TGDefect User Guide Revisions
- APPENDIX - TGDetect Collectors
- APPENDIX - TGDetect Built-in History Log (QHST) Rules
- APPENDIX - TG Fix
- APPENDIX - TG Management
- APPENDIX - TG Save and Restore
APPENDIX - TGDetect Revisions

This section includes enhancement by version.

- Version 2.4 - TGDetect User Guide Revisions
- Version 2.3 - TGDetect User Guide Revisions
- Version 2.2 - TGDefect User Guide Revisions
- Version 2.1 - TGDefect User Guide Revisions
Version 2.4 - TGDetect User Guide Revisions

Enhancements

- Addition of SEIM batch configuration details
- SIEM Batch Process enhanced support Message Queues (*MSGQ) and History Log (*QHST)
Version 2.3 - TGDetect User Guide Revisions

This release includes the following enhancement:

**Managing Monitors**

You can now enable monitors from the *last process time* or the *current time*.

See [Manage Monitors](#) for details.
Version 2.2 - TGDefect User Guide Revisions

This release includes the following enhancements:

**History (QHST) Log Monitor**

- Added Built-in History Log Monitor rules
  These built-in rules ship with the product and assist the security admin in creating notifications for important system events (e.g., license expiration, etc.)

- Added the Monitor MSGs Need Reply Only feature to the History Log Monitor rule criteria
  This feature allows you to limit notifications for only messages that require the admin to reply (C, G, D, F).

**Message Queue Monitor**

- Added the Monitor MSGs Need Reply Only feature to the Message Queue Monitor rule criteria
  This feature allows you to limit notifications for only messages that require the admin to reply (C, G, D, F).
Version 2.1 - TGDefect User Guide Revisions

This release includes the following enhancements:

- Addition of minimum severity to history log rule criteria
- Addition of minimum severity to message queue rule criteria
- Message queue filtering with the addition of nesting
## APPENDIX - TGDetect Collectors

<table>
<thead>
<tr>
<th>Collector ID</th>
<th>Collector Name</th>
<th>Collector Category</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_ESCAL_ACC_CONTROLS</td>
<td>Access Escalation Access Controls</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_DEFAULTS</td>
<td>Access Escalation Defaults</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_ENTITLEMENTS</td>
<td>Access Escalation Entitlements</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_FILE_EDITORS</td>
<td>Access Escalation File Editors</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ACCESS_ESCAL_USAGE</td>
<td>Access Escalation Usage</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTH_USERS_VIA_AUTH_LISTS</td>
<td>Authorized Users through Authorization Lists</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_ALI</td>
<td>Authority Collection Report (*ALL)</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_IFS</td>
<td>Auth Collection For Objects IFS Report</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COL_OBJECT</td>
<td>Auth Collection For Objects Native Report</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COLLECTION</td>
<td>Authority Collection Data</td>
<td>Journal</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_COMPLIANCE</td>
<td>Authority Compliance</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>AUTHORITY_LIST</td>
<td>Authority List Data</td>
<td>System</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_3RD_PARTY_FILE</td>
<td>Blueprint 3rd Party Integration File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_AUTH_SETTINGS_FILE</td>
<td>Blueprint Authority List Settings File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_MASTER</td>
<td>Blueprint Master</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_NON_COMPLIANCE_USER</td>
<td>Blueprint Non-Compliance User Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_OBJECT_AUTH_FILE</td>
<td>Blueprint Object Authority File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_PARAMETER_FILE</td>
<td>Blueprint Parameter File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>BLUEPRINT_PERMISSION_FILE</td>
<td>Blueprint Permission File</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_COMMANDS</td>
<td>Commands Allowed/Rejected via Command Security</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_CONF_SETTINGS</td>
<td>Command Security Config Settings</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_PARAM_LEVEL</td>
<td>Command Security Paramater Level</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CMD_SEC_RULES</td>
<td>Command Security Config Settings</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>CONTROLLER.Attached_Devices</td>
<td>Command Security Parameter Level</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td>CONTROLLER.Description_Data</td>
<td>Controller Description Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATA.Area_Auditing</td>
<td>Audit data area changes</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE.Access</td>
<td>Database File Access</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE.Auditing</td>
<td>Monitor Database changes</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE.Content</td>
<td>Database Content</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE.Field_ACTIVITY</td>
<td>Database Field Activity</td>
<td>Resources</td>
<td>IBMi</td>
</tr>
<tr>
<td>DATABASE.Operations</td>
<td>Database Operations</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.ACT.History</td>
<td>Detect Activity History</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Defaults</td>
<td>Detect Defaults</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Cmd.Rules</td>
<td>Command Monitor Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.JRN.Seim.Rules</td>
<td>Journal Monitor Rules for SEIM</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.JRNMon.Alerts</td>
<td>Journal Monitor Alerts</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.JRNMon.Rules</td>
<td>Journal Monitor Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Mon.Master</td>
<td>Monitor Master</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Msq.Cmd.Alr</td>
<td>Message Queue and Command Alerts</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Msq.Rules</td>
<td>Message Queue Rules</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Seim.Providers</td>
<td>SEIM Providers</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DET.Snmp.Trp.Pckg</td>
<td>SNMP Trap Packages</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>DEVICE.Description_APPC</td>
<td>Device Description APPC Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DEVICE.Description_Data</td>
<td>Device Description Information</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>DTBase.Operations_JRN</td>
<td>Database Operations by Journal</td>
<td>N/A</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT.Database.Field</td>
<td>Encryption Database Field Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT.Database.File</td>
<td>Encryption Database File Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT.Database.Filter</td>
<td>Encryption Database File Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPT.Database.Rules</td>
<td>Encryption Database Rule Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>ENCRYPTION.Defaults</td>
<td>Encryption Defaults</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>EXIT.Points</td>
<td>Display Exit Point Data</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>FIELD.Authority</td>
<td>Display Field Level Authorities</td>
<td>Object</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS.Attributes</td>
<td>Display the attributes for the IFS objects</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>Resource/Profile</td>
<td>Description</td>
<td>Type</td>
<td>Platform</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>IFS_AUTHORITIES</td>
<td>Display the public and private authorities associated with the object</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_CONTENT</td>
<td>IFS Content</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_JOURNALING</td>
<td>Display extended journaling information for the IFS object</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>IFS_STATUS</td>
<td>Display status information about an IFS file</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>INACTIVITY_DISCONNECTS</td>
<td>Inactivity Disconnections</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>INCOMING_TRANSACTIONS</td>
<td>Incoming Transactions</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_CONFIGURATION_SETTINGS</td>
<td>ISL Configuration Settings</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_DISCONNECT_OPTIONS</td>
<td>ISL Disconnect Options</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>ISL_RULES</td>
<td>ISL Inclusion Exclusion Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_ACTIVITY_DETAILS</td>
<td>Job Activity Details</td>
<td>Log</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_ACTIVITY_SUMMARY</td>
<td>Job Activity Summary</td>
<td>Log</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOB_DESCRIPTIONS</td>
<td>Job Description Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AD</td>
<td>Object Auditing Attribute Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AF</td>
<td>Authority Failures</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AP</td>
<td>Programs that Adopt Authority were Executed</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AU</td>
<td>EIM Attribute Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_AX</td>
<td>Row and Column Access Control</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CA</td>
<td>Authorization List or Object Authority Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CD</td>
<td>Commands Executed</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL.CO</td>
<td>Create Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CP</td>
<td>User Profile Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CQ</td>
<td>Change Request Descriptor Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CU</td>
<td>Cluster Operation</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL.CV</td>
<td>Connection Verification</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CY</td>
<td>Cryptographic Configuration Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DI</td>
<td>LDAP Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DO</td>
<td>Delete Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_DS</td>
<td>Changes to Service Tools Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_EV</td>
<td>Environment Variable Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_GR</td>
<td>Exit Point Maintenance Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_CODE</td>
<td>JOURNAL_DESCRIPTION</td>
<td>JOURNAL_TYPE</td>
<td>JOURNAL_VENDOR</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>JOURNAL_GS</td>
<td>Socket Descriptor Details</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IM</td>
<td>Intrusion Monitor Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IP</td>
<td>Inter-process Communication Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IR</td>
<td>Actions to IP Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_IS</td>
<td>Internet Security Management Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_JD</td>
<td>Job Descriptions – USER Parameter Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_JS</td>
<td>Job Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_KF</td>
<td>Key Ring File Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_LD</td>
<td>Directory Link, Unlink, and Search Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M0</td>
<td>Db2 Mirror Setup Tools</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M6</td>
<td>Db2 Mirror Communication Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M7</td>
<td>Db2 Mirror Replication Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M8</td>
<td>Db2 Mirror Product Services</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_M9</td>
<td>Db2 Mirror Replication State</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ML</td>
<td>OfficeVision Mail Services Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_NA</td>
<td>Network Attribute Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ND</td>
<td>Directory Search Violations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_NE</td>
<td>APPN Endpoint Filter Violations</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O1</td>
<td>Single Optical Object Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O2</td>
<td>Dual Optical Object Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_O3</td>
<td>Optical Volume Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OM</td>
<td>Object Management Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OR</td>
<td>Objects Restored</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_OW</td>
<td>Object Ownership Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PA</td>
<td>Program Changes to Adopt Owner Authority</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PF</td>
<td>PTF Operations</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PG</td>
<td>Primary Group Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PO</td>
<td>Printer Output Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PS</td>
<td>Swap Profile Events</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL PU</td>
<td>PTF Object Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_PW</td>
<td>Invalid Sign-on Attempts</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RA</td>
<td>Authority Changes to Restored Objects</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RJ</td>
<td>Job Descriptions that Contain User Profile Names were Restored</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------</td>
<td>-----</td>
</tr>
<tr>
<td>JOURNAL_RO</td>
<td>Ownership Changes for Restored Objects</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RP</td>
<td>Programs Restored that Adopt Owner Authority</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RQ</td>
<td>Change Request Descriptors Restored</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RU</td>
<td>Authority Restored for User Profiles</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_RZ</td>
<td>Primary Group Changes for Restored Objects</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SD</td>
<td>System Directory Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SE</td>
<td>Subsystem Routing Entry Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SF</td>
<td>Spooled File Actions</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SG</td>
<td>Asynchronous Signals Processed</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SK</td>
<td>Secure Socket Connections</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SM</td>
<td>Systems Management Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SO</td>
<td>Server Security User Information Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ST</td>
<td>Service Tools Actions</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_SV</td>
<td>System Values Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VA</td>
<td>Access Control List Changes</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VC</td>
<td>Connections Started, Ended, or Rejected</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VF</td>
<td>Close Operations on Server Files</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VL</td>
<td>Exceeded Account Limit Events</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VN</td>
<td>Network Log On and Off Events</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VO</td>
<td>Actions on Validation Lists</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VP</td>
<td>Network Password Errors</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VR</td>
<td>Network Resource Accesses</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VS</td>
<td>Server Sessions Started or Ended</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VU</td>
<td>Network Profile Changes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_VV</td>
<td>Service Status Change Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_X0</td>
<td>Network Authentication Events</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_X1</td>
<td>Identity Token Events</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_XD</td>
<td>Directory Server Extensions</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_YC</td>
<td>DLO Object Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_YR</td>
<td>DLO Object Reads</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>JOURNAL_ZC</td>
<td>Object Changes</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>Resource</td>
<td>Configuration</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----</td>
</tr>
<tr>
<td>JOURNAL_ZR</td>
<td>Object Reads</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KEYSTORE_DATA</td>
<td>KeyStore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LIBRARY_STAT</td>
<td>Library Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINE_DESCRIPTION_DATA</td>
<td>Line Description Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MESSAGE_QUEUE</td>
<td>Message Queue Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MESSAGE_QUEUE_DATA</td>
<td>Message Queue Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETSERVER_CONFIG</td>
<td>NetServer Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETSERVER_SHARES</td>
<td>NetServer Shares</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_ATTRIBUTES</td>
<td>Network Attribute Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_CONNECTIONS</td>
<td>Network Connections Ipv4 and Ipv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_EXIT_CONFIG</td>
<td>Exit Point Configuration Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_INTERFACE_IPV4</td>
<td>Network Interface Data Ipv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_INTERFACE_IPV6</td>
<td>Network Interface Data Ipv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_ROUTE_IPV4</td>
<td>Network Route Data Ipv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_ROUTE_IPV6</td>
<td>Network Route Data Ipv6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_SERVER_DESCRIPTIONS</td>
<td>Network Server Description Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_SVR_ENCRYPT_STATUS</td>
<td>Network Server Encryption Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TCP/IP_V4</td>
<td>TCP/IP Ipv4 Stack Attributes/Remote Exit Rule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TCP/IP_V6</td>
<td>TCP/IP Ipv6 Stack Attributes/Remote Exit Rule</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_CENTRAL</td>
<td>Central Server Transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_COMMAND</td>
<td>Remote Command Transactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_DATABASE</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_DATAQ</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_DDM</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_FILE</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_FTP_REXEC</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_PRINTER</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_SHOWCASE</td>
<td>Network Trans Showcase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_SIGNON</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETWORK_TRANS_TELNET</td>
<td>Remote Exit Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
<td>IBMi</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>OBJECT_AUTHORITY</td>
<td>Display Object Authority</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>OBJECT_DETAILS</td>
<td>Display Object Details</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>OBJECT_STAT</td>
<td>Object/File Statistics</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>OUTPUT_QUEUE</td>
<td>Output Queue Information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>PRODUCT_INFO</td>
<td>Basic Information about a software product</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>PROFILE_COMPLIANCE</td>
<td>Profile Compliance Data</td>
<td>Profile</td>
<td></td>
</tr>
<tr>
<td>PROFILE_INACTIVITY_SETTNGS</td>
<td>Profile Inactivity Settings</td>
<td>Profile</td>
<td></td>
</tr>
<tr>
<td>PROFILE_MANAGER_DEFAULTS</td>
<td>Profile Manager Defaults</td>
<td>Profile</td>
<td></td>
</tr>
<tr>
<td>PROGRAM_ADOPT</td>
<td>Programs that Adopt Authority</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>PROGRAM_REFERENCE_DATA</td>
<td>Program Reference Data</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>PTF_DATA</td>
<td>Program Temporary Fix Data</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QHST_MSG_INFO</td>
<td>QHST History Log Information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.ACTIVE_JOB_INFO</td>
<td>Active job information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.DATA_QUEUE_ENTRIES</td>
<td>Data Queue Entries</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>QSYS2.DRDA_AUTHENTICATION</td>
<td>DRDA and DDM User access</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.EXIT_POINT_INFO</td>
<td>Exit Point Information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.EXIT_PROGRAM_INFO</td>
<td>Exit Program Information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2_FUNCTION_INFO</td>
<td>Function usage identifiers</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2_FUNCTION_USAGE</td>
<td>Function usage configuration details.</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.GROUP_PTF_INFO</td>
<td>Group PTFs Information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.JOURNAL_INFO</td>
<td>Journal and remote journal information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.JOURNALED_OBJECTS</td>
<td>Journal object information</td>
<td>Resource</td>
<td></td>
</tr>
<tr>
<td>QSYS2.LICENSE_INFO</td>
<td>Products license information</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEDIA_LIBRARY_INFO</td>
<td>Media Library Status details</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEMORY_POOL</td>
<td>Memory pool details</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.MEMORY_POOL_INFO</td>
<td>Active memory pools</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>QSYS2.MESSAGE_QUEUE_INFO</td>
<td>Message Queue</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Object Name</td>
<td>Description</td>
<td>Type</td>
<td>Platform</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>QSYS2.NETSTAT_JOB_INFO</td>
<td>IPv4 and IPv6 network connection details.</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.OBJECT_LOCK_INFO</td>
<td>Object lock information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.OUTPUT_QUEUE_ENTRIES</td>
<td>Spooled file in output queue</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.RECORD_LOCK_INFO</td>
<td>Record lock information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.REPLY_LIST_INFO</td>
<td>Current job's reply list entry information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SCHEDULED_JOB_INFO</td>
<td>Job Schedule Entry information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SERVER_SBS_ROUTING</td>
<td>Alternate subsystem configurations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SERVER_SHARE_INFO</td>
<td>Server Share Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SOFTWARE_PRODUCT</td>
<td>Server Software Product information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLS</td>
<td>Permissions or column mask defined</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSCONTROLSDEP</td>
<td>Dependencies of row permissions and column masks</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSDISKSTAT</td>
<td>Disk Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSTEM_STATUS_INFO</td>
<td>Partition information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.SYSTMPSTG</td>
<td>IBM i temporary storage pool detail</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.USER_INFO</td>
<td>User Profile Information</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>QSYS2.USER_STORAGE</td>
<td>Storage usage by user profile</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>REMOTE_TRAN_SUMMARY_BY_SERVER</td>
<td>Remote Summary Server</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>REMOTE_TRAN_SUMMARY_BY_USER</td>
<td>Remote Summary User</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_COMPLIANCE_DATA</td>
<td>Resource Manager Authority Out of compliance data</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_CONFIG</td>
<td>Resource Manager Configuration</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_SCHEMADETAILS</td>
<td>Resource Manager Authority Schema Details</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>RSC_MGR_SCHEMA_HEADER</td>
<td>Resource Manager Authority Schema Header</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SENSITIVE_DATABASE_CONTENT</td>
<td>Sensitive Database Content</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>SERVICE_TOOL_SECURITY_ATTR</td>
<td>Service Tool Security Attributes</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>SERVICE_TOOL_USERS</td>
<td>Service Tool User Data</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>Table Name</td>
<td>Description</td>
<td>Type</td>
<td>Vendor</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------</td>
</tr>
<tr>
<td>SOCKET_SUMMARY_BY_SERVER</td>
<td>Socket Summary by Server</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_SUMMARY_BY_USER</td>
<td>Socket Summary by User</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_TRAN_RULES</td>
<td>Socket Rules</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOCKET_TRANSACTIONS</td>
<td>Socket Transactions</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>SOFTWARE_RESOURCES</td>
<td>Installed Software Resources Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_AUTOSTART</td>
<td>Subsystem Autostart Jobs</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_COMMUNICATIONS</td>
<td>Subsystem Communication Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_INFORMATION</td>
<td>Subsystem Information Details</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_JOB_QUEUE</td>
<td>Subsystem Job Queue</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_POOL_DATA</td>
<td>Subsystem Pool Data</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_PRESTART</td>
<td>Subsystem Prestart Jobs</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_REMOTE</td>
<td>Subsystem Remote Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_ROUTING</td>
<td>Subsystem Routing Entries</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_WORKSTATION_NAMES</td>
<td>Subsystem Workstation Names</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SUBSYSTEM_WORKSTATION_TYPES</td>
<td>Subsystem Workstation Types</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_CONFIG</td>
<td>System Value Configuration</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_DEFAULT</td>
<td>System Value Default</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYS_VAL_VALID</td>
<td>System Value Default</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCOLAUTH</td>
<td>Privileges Granted on a Column</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLS</td>
<td>Permission or Column Mask Defined</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLSDEP</td>
<td>Dependencies of Row Permissions and Column Masks</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSCONTROLSDEP</td>
<td>Privileges Granted on a Row</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSFIELDS</td>
<td>Columns with Field Procedures</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSPACKAGEAUTH</td>
<td>Privileges Granted on a Package</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSPROGRAMSTAT</td>
<td>Program, Service Program, and Module with SQL Statements</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSROUTINEAUTH</td>
<td>Privileges Granted on a Routine</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSSCHEMAMAUTH</td>
<td>Privileges Granted on a Schema</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSSQUENCEAUTH</td>
<td>Privileges Granted on a Sequence</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTABAUTH</td>
<td>Privileges Granted on a Table or View</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>Table Name</td>
<td>Description</td>
<td>Category</td>
<td>Vendor</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>SYSTABLESTAT</td>
<td>Table Statistics Include all Partitions and Members</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTEM_VALUES</td>
<td>Display System Value Data</td>
<td>System</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTOOLS.GROUP_PTF_CURRENCY</td>
<td>PTF Groups Installed per IBM Recommendations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSTOOLS.GROUP_PTFDETAILS</td>
<td>PTFs within PTF Groups Installed per IBM Recommendations</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSUDTAUTH</td>
<td>Privileges Granted on a Type</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSVARIALEAUTH</td>
<td>Privileges Granted on a Global Variable</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>SYSXSROBJECTAUTH</td>
<td>Privileges Granted on an XML Schema</td>
<td>Configuration</td>
<td>IBMi</td>
</tr>
<tr>
<td>TIMOBJINF</td>
<td>Object Information</td>
<td>Resource</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_NETWORK_GROUPS</td>
<td>TG Network Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_OBJECT_GROUPS</td>
<td>TG Object Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_OPERATION_GROUPS</td>
<td>TG Operation Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>TG_USER_GROUPS</td>
<td>TG User Groups</td>
<td>Network</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_OBJECT_AUTHORITIES</td>
<td>User Profile Object Authorities</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PRF_VIA_BLUEPRINT</td>
<td>User Profile via Blueprint</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_ACTIVITY</td>
<td>User Profile Activity</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_ARCHIVE</td>
<td>User Profile Archive</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILE_EXCLUSIONS</td>
<td>User Profile Exclusions</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
<tr>
<td>USER_PROFILES</td>
<td>Display User Profile Data</td>
<td>Profile</td>
<td>IBMi</td>
</tr>
</tbody>
</table>
## APPENDIX - TGDetect Built-in History Log (QHST) Rules

The History Log Monitor contains the following pre-defined rules:

<table>
<thead>
<tr>
<th>Rule ID</th>
<th>Rule Name</th>
<th>Create notifications about the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage_Objects</td>
<td>Damage Objects</td>
<td>Detection of error or damage to object(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following are the out-of-the-box message IDs available for <strong>Damage_Objects</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPFAFA0 - Errors detected on MSF internal message index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPFAFA1 - Errors detected on MSF internal message queue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPFA09F - Object damaged. Object is &amp;1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPFBB83 - Internal cluster object damaged</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPF0C19 - Damage occurred on object &amp;1 in library &amp;2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: This is not an exhaustive list of message IDs–just a sample. Access the History Log Monitor to view the complete list.</td>
</tr>
<tr>
<td>Hardware_Failures</td>
<td>Hardware failures and Critical conditions</td>
<td>Detection of hardware failures or critical conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following are the out-of-the-box message IDs available for <strong>Hardware_Failures</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPA3576 - Error during PTF request. Press Help before replying</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPA5201 - Hardware failure on device &amp;3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPA578C - Controller &amp;24 online &amp;23 failed. Probable insufficient resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPFAD93 - APPC failure. Failure code is &amp;3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPP8988 - A critical system hardware problem has occurred. Critical Message Handler has been run</td>
</tr>
<tr>
<td>Invalid_Signon</td>
<td>Invalid Signon Attempts</td>
<td>Detection of invalid sign-on attempts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following are the out-of-the-box message IDs available for <strong>Invalid_Signon</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPF1393 - User profile &amp;2 has been disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPF1397 - Subsystem &amp;1 varied off work station &amp;3 for user &amp;8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CPF2234 - Password from device &amp;1 not correct for user &amp;2</td>
</tr>
<tr>
<td>Licensing Issues</td>
<td>Description</td>
<td>Example Message IDs</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| **Licensing**    | Detection of licensing expirations, limitations, etc. | - CPF9E7A - IBM i usage limit exceeded - operator action required  
- CPF9E7B - Cannot release different number of uses than requested  
- CPF9E7C - IBM i grace period expired  
- CPF9E7E - IBM i license key not valid in &8 days on &9  
- CPF9E70 - Grace period expired. Requesting user already added  
- CPF9E72 - Usage limit of &4 exceeded. Grace period expires in &6 days on &5 |

**Note**: This is not an exhaustive list of message IDs–just a sample. Access the History Log Monitor to view the complete list.

<table>
<thead>
<tr>
<th>Multipl_e_Rec_eivers</th>
<th>Description</th>
<th>Example Message IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multiple_Receivers</strong></td>
<td>Detection of multiple receivers</td>
<td>- CPC7011 - Journal receiver &amp;1 created in library &amp;2</td>
</tr>
</tbody>
</table>

**Tip**: Use the alert criteria defined for the Multiple_Receivers rule to set a threshold. For example, if you set the threshold at 4, then TGDetect sends the designated recipient a notification once four receivers are detected.

<table>
<thead>
<tr>
<th>Qsecof_r_Signon</th>
<th>Description</th>
<th>Example Message IDs</th>
</tr>
</thead>
</table>
| **QSECOFR Signon** | Detection of signon by a high-profile (QSECOFR) | - CPF1124 - Job &3/&2/&1 started on &18 at &19 in subsystem &8 in &9. Job entered system on &20 at &21.&17  
- CPIAD0B - *SIGNON server job &3/&2/&1 processing request for user &4 on &5 in subsystem &6 in &7  
- CPIAD09 - User &4 from client &8 connected to job &3/&2/&1 in subsystem &6 in &7 on &5  
- CPIAD12 - Servicing user profile &1 from client &2 |

<table>
<thead>
<tr>
<th>QAUDCTL_Changes</th>
<th>Description</th>
<th>Example Message IDs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QAUDCTL_Changes</strong></td>
<td>Detection of change to changes to system values</td>
<td>- CPF180F - System value &amp;1 changed</td>
</tr>
</tbody>
</table>

**Note**: The following are the out-of-the box message IDs available for **Licensing**: **Multiple_Receivers**: **Qsecofr_Signon**: **QAUDCTL_Changes**:
<table>
<thead>
<tr>
<th>Storages Issues</th>
<th>Storage Issues</th>
<th>Detection of storage limit capacity issues</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The following are the out-of-the-box message IDs available for <strong>Storage_Issues</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPFA08F - User profile storage limit exceeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPFA80A - Data queue &amp;1 is full</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPFB515 - Not enough storage in machine pool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPFB569 - Main storage allocation failure occurred</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF090A - Temporary storage threshold reached</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF950A - Storage limit exceeded for data queue &amp;1 in &amp;2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPI1468 - System job tables nearing capacity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subsystem Messages</th>
<th>Subsystem Messages</th>
<th>Detection of subsystem failures (i.e., cannot open, start, or find)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The following are examples of out-of-the-box message IDs available for <strong>Subsystem_Messages</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF1011 - Start subsystem failed for SBSD &amp;1 in library &amp;2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF117A - Subsystem &amp;1 cannot start autostart job &amp;2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF1171 - Subsystem &amp;1 cannot find file &amp;2 in library &amp;3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF1172 - Subsystem &amp;1 cannot open file &amp;2 in library &amp;3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: This is not an exhaustive list of message IDs--just a sample. Access the History Log Monitor to view the complete list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Events</th>
<th>System events and subsystem activity</th>
<th>Detection of system and system activities that impact security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The following are examples of out-of-the-box message IDs available for <strong>System_Events</strong>:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPFAD10 - An error was detected in the exit program &amp;1 in library &amp;2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF0849 - Space addressing violation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF0927 - Subsystem &amp;1 ended</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF0934 - IPL completed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- CPF1103 - Subsystem &amp;1 started</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: This is not an exhaustive list of message IDs--just a sample. Access the History Log Monitor to view the complete list.</td>
</tr>
</tbody>
</table>
APPENDIX - TG Fix

The TG Fix tool allows you to install fixes via the TG menu quickly and easily. This feature also includes verification features that ensure the fix is installed properly.

See also

Working with TG Fix
APPENDIX - TG Management

The TG Management tool allows you to configure TG product administrative elements (e.g., licensing, user authorization, report output formats, etc.).

See also

Working with TG Management
APPENDIX - TG Save and Restore

The **TG Save and Restore** tool allows you to save the configuration of a specific instance of TGSecure or TGAudit. Once you save a configuration, you can then use that saved configuration file to do the following:

- Create a back-up (archive) of the current configuration to be used later to restore the configuration of an agent (server)
- Create multiple instances with identical configuration

A saved file stores the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules (i.e., Socket Rules, Exit Rules, etc.)

**See also**

*Working with the TG Save and Restore*