NetIQ Security Solutions for IBM i
TGDetect 2.4
User Guide
Revised September 2021

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© 2021 Trinity Guard LLC. All rights reserved.

1. What's New . . . 5
2. TGDetect Introduction . . . 6
2.1 Features . . . 7
3. Getting Started . . . 9
3.1 Log Into TGDetect . . . 11
3.2 Working with TGDetect . . . 12
4. Defaults . . . 13
4.1 Working with TGDetect Defaults . . . 14
4.2 Display TGDetect Defaults . . . 15
4.3 Manage TGDetect Defaults . . . 16
4.4 Run TGDetect Default Setting Reports . . . 20
5. Monitors . . . 22
5.1 Working with Monitors . . . 23
5.1.1 Display Monitors . . . 24
5.1.2 Manage Monitors . . . 26
5.1.3 Run Monitor Master Reports . . . 29
5.2 Command Monitor . . . 31
5.2.1 Working with Command Monitor . . . 32
5.2.2 Display Command Monitor Rules . . . 33
5.2.3 Display Command Monitor Rule Criteria . . . 35
5.2.4 Display Command Monitor Alerts . . . 37
5.2.5 Display Command Monitor Activity Log . . . 39
5.2.6 Manage Command Monitor Rules . . . 40
5.2.7 Manage Command Monitor Rule Criteria . . . 42
5.2.8 Manage Command Monitor Alerts . . . 44
5.2.9 Run Command Monitor Reports . . . 47
5.3 History Log Monitor . . . 51
5.3.1 Working with History Log Monitor . . . 52
5.3.2 Display History Log Rules . . . 53
5.3.3 Display History Log Rule Criteria . . . 55
5.3.4 Display History Log Alerts . . . 57
5.3.5 Display History Log Activity Log . . . 59
5.3.6 Manage History Log Rules . . . 60
5.3.7 Manage History Log Rule Criteria . . . 62
5.3.8 Manage History Log Alerts . . . 67
5.3.9 Run History Log Reports . . . 70
5.4 Journal Monitor . . . 71
5.4.1 Working with Journal Monitor . . . 72
5.4.2 Display Journal Monitor Rules . . . 73
5.4.3 Display Journal Monitor Rule Criteria . . . 76
5.4.4 Display Journal Monitor Alerts . . . 77
5.4.5 Display Journal Monitor Activity Log . . . 78
5.4.6 Manage Journal Monitor Rules . . . 79
5.4.7 Manage Journal Monitor Rule Criteria . . . 81
5.4.8 Manage Journal Monitor Alerts . . . 83
5.4.9 Run Journal Monitor Reports . . . 85
5.5 Message Queue Monitor . . . 88
5.5.1 Working with the Message Queue Montior . . . 89
5.5.2 Display Message Queue Rules . . . 90
5.5.3 Display Message Queue Rule Criteria . . . 92
5.5.4 Display Message Queue Alerts . . . 94
5.5.5 Display Message Queue Activity Log . . . 95
5.5.6 Manage Message Queue Rules . . . 96
5.5.7 Manage Message Queue Rule Criteria . . . 98
5.5.8 Manage Message Queue Alerts . . . 103
5.5.9 Run Message Queue Reports . . . 106
5.6 SIEM Monitor . . . 110
5.6.1 Working with SIEM Monitor . . . 111
5.6.2 Display SIEM Monitor Rules . . . 112
5.6.3 Display SIEM Monitor Rule Criteria . . . 114

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
11.1.4 Version 2.1 - TGDefect User Guide Revisions . . . 167
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

Version 2.4 - TGDetect User Guide Revisions
Enhancements • Addition of SEIM batch configuration details • SIEM Bach Process enhanced support Message Queues (*MSGQ) and History Log (*QHST)

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.

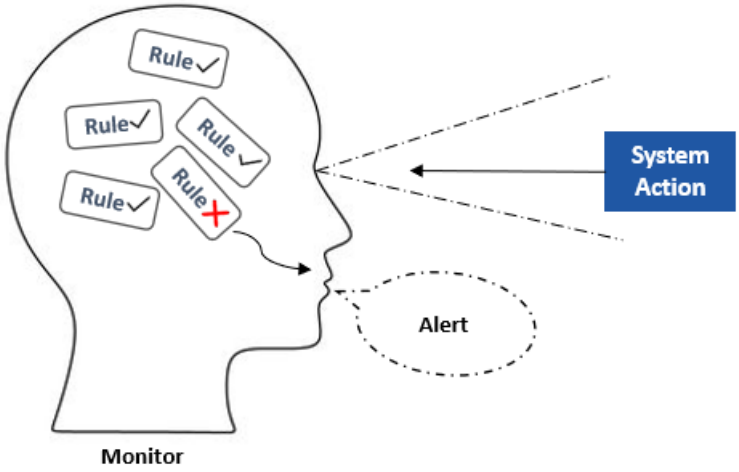
See also

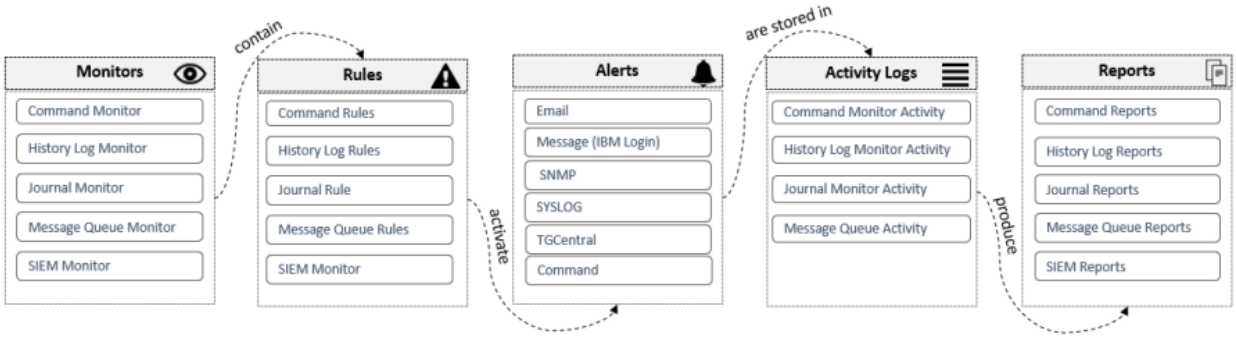
What's New

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:

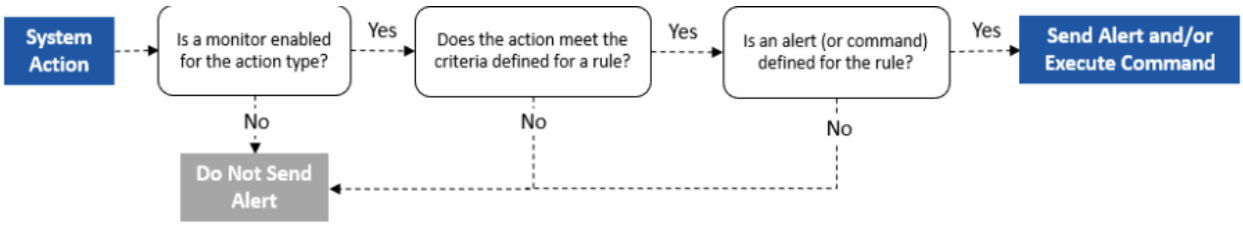
- Actions
- Process Flow
- Implementation Tasks

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



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.

Step	Description
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.

4	**Create Monitor Rules** 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 Working with Monitor Rules for additional information.
5	**Create Alerts** To define the designated recipient for a notification, you must create alerts. See Working with Monitor Alerts for additional information.
6	**Display Activity Logs** To view the alerts generated for a specific monitor, access the activity log for that monitor. See Working with Monitor Activity Logs for additional information.
7	**Run Reports** Run reports to monitor activity and track changes. See Working with Monitor Reports for additional information.

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 to 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**.

Field	Description
History Log	Enter (in seconds) how often to check the history log monitor for alerts that required sending
Message Queue	Enter (in seconds) how often to check the message queue monitor for alerts that required sending
Real-time Journal	Enter (in seconds) how often to check the journal monitor for alerts that required sending

> **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**.

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

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

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**.

Field	Description
Audit Journal	Enter the journal in which to store alert data **Note**: The default audit journal for TG products is TGJRN. This journal resides in the TGDATA library.

Audit Journal Library	Enter the library in which the journal is stored
Audit Configuration Changes	Enter one of the following: **Y** - Enable tracking of changes **N** - Disable tracking of changes **Tip**: Set this flag to **Y** to 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.

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

3) Press **Enter.**

Configure SIEM Batch

Use this task to configure SIEM Batch details.

Note: You must configure SIEM batch details to enable sending events in batch mode.

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.

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

Stop Subsystem

Use this task to stop 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.

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 TGDetect Default Setting Reports

Use this task to generate the following reports:

- Access the TGDetect Reports Interface
- Run Default Settings Report
- Run Default Settings 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 Default Settings Report

Use this report to display the list of default settings.

To run the Default Settings 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 **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.

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

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 product 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:

Field	Description
Monitor Name	Name of the object you want to monitor
Monitor Library	Library you want to monitor

Type	***MSGQ** - Message queue monitor **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.
Description	A short description identifying the purpose of the monitor

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 know 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).

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

Field	Description
Rule ID	Unique Identifier assigned to command rule
Rule Name	Name assigned to the rule
Calendar	Name of the calendar that defines when the rule is applicable
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 - 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).

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

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

Field	Description
Rule ID	Unique ID assigned to the rule for which you are displaying criteria
Rule Name	Name assigned to the rule for which you are displaying criteria
Command Name	Command for which you want to establish a rule
Command Library	Library in which you want to monitor using the rule
User Name	User/user group you want to monitor using the rule **Tip**: Enter ***ALL** to monitor all users.
Description	Description of the criteria

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.

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 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

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).

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

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

Field	Description
Rule ID	Unique ID assigned to the rule for which you are displaying alerts
Rule Name	Name assigned to the rule for which you are displaying alerts
Alt Seq	The sequence in which alerts are sent **Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.
Alert Type	Type of alert *__EMAIL__ - Send an email alert to a specific user/group *__MSG__ - Send a system message (message that appears when a user logs into the system) *__CMD__ - Execute a command *__SYSLOG__ - Send a notification to the system archive *__EMAILDIST__ - Send an email alert to a specific user (legacy IBM method of sending email alerts) *__TGCENTRAL__ - Send a notification to TGCentral
Alert Details	Recipient details
Message to Send	Text included in the notification sent to the designated recipient
Alert Criteria - #Events	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 **Freq** field.
Alert Criteria - Freq	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.

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).

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

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

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

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).

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

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.

Field	Description
Rule ID	Enter a unique identifier for the command rule
Rule Name	Enter a name for the command rule
Calendar	Enter the name of the calendar that defines when the rule is applicable **Tip**: Enter ***NONE** if no calendar is applicable.

> **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).

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

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.

Field	Description
Command Name	Enter the command for which you want to establish a rule
Command Library	Enter the library in which you want to monitor using the rule
Command User	Enter the user/user group you want to monitor using the rule **Tip**: Enter ***ALL** to monitor all users.

> **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).

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

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.

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

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.

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.

> **Note**: The criteria allow you to limit the data returned in the report.

> **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 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.

Field	Description
Rule ID	Unique Identifier assigned to history log rule **Note**: See History Log Rules for a description of the built-in rules that ship with TGDetect.
Rule Name	Name assigned to the rule
Calendar	Name of the calendar that defines when the rule is applicable
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** 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.
>
> - Ads 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).

3) Press **Enter**. The **Work with Rules - QSYS/QHST** 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.

Field	Description
Rule ID	Unique ID assigned to the rule for which you are displaying criteria
Rule Name	Name assigned to the rule for which you are displaying criteria
Minimum Severity	The rule severity level that must be met to trigger a message (notification)
MSGID	Unique ID assigned to the message rule criteria
Message File	File in which the message rule resides
Message Library	Library in which the message rule resides
Description	Description of rule
Omit or Select	Identifies whether the rule criteria 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)
Field Compare	Identifies any field value filters
Reply	Reply sent to the recipient

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 - QSYS/QHST** 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 - 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.

Field	Description
Rule ID	Unique ID assigned to the rule for which you are displaying alerts
Rule Name	Name assigned to the rule for which you are displaying alerts
Alt Seq	The sequence in which alerts are sent **Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.
Alert Type	Type of alert ***EMAIL** - Send an email alert to a specific user/group ***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral
Alert Details	Recipient details
Message to Send	Text included in the notification sent to the designated recipient
Alert Criteria - #Events	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 **Freq** field.
Alert Criteria - Freq	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.

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.

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

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).

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

Add History Log Rule

Use this task to add a history log rule.

To add a history rule

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

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

3) Complete the following fields.

Field	Description
Rule ID	Enter a unique identifier for the history log rule
Rule Name	Enter a name for the history log rule
Calendar	Enter the name of the calendar that defines when the rule is applicable **Tip**: Enter ***NONE** if no calendar is applicable.

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

4) Press **Enter** twice.

Edit History Log Rule

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 a delete 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.

Field	Description
Message ID	Enter a unique ID for the message rule
Message File	Enter the file in which the message rule resides
Message File Library	Enter the library in which the message rule resides

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.

Tip: This feature is available only when variable fields (which appear with & placeholders) are present in the message description. See the following examples:

- Message description with a single variable field: "Hardware failure on device **&1**"
- Message description with multiple variable fields: "Controller **&1** on line **&2** failed"
- Message description with no variable fields: "Error during PTF request"

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.

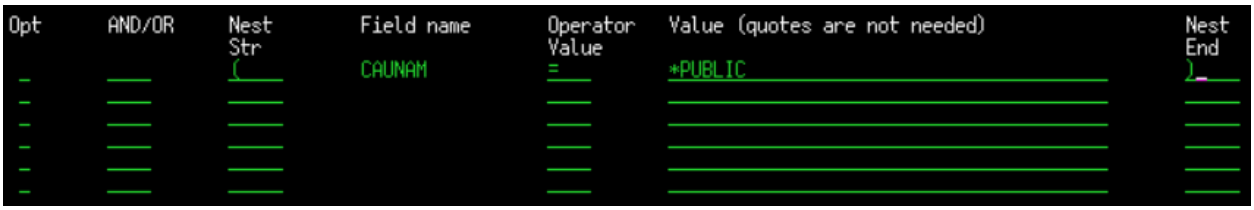
Tip: If the dialog contains no compare fields (blank), then this feature is not available for the selected message.

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.

> **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:

Field	Description
Monitor Messages Requiring Reply Only	Enter one of the following: ***NO** - Send notifications for all message in the queue ***YES** - Send notifications for only messages that required a reply **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 - 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.

Field	Description
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.

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

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. **Tip**: This option is useful for setting thresholds that must be met before an alert is triggered.
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.

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.

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

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** 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 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).

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

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

Field	Description
Alt Seq	The sequence in which alerts are sent **Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.
Alert Type	Type of alert ***EMAIL** - Send an email alert to a specific user/group ***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral
Alert Details	Recipient details
Message to Send	Text included in the notification sent to the designated recipient
Alert Criteria - #Events	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 **Freq** field.
Alert Criteria - Freq	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.

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).

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

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.

Field	Description
Activity Type	Type of alert: *__CMD__ - Command executed *__EMAIL__- Email sent *__MSG__ - System (login) message queued *__SYSLOG__ - Syslog communication initiated
Activity Status	Status of alert
Activity Date	Date on which the alert was triggered
Activity Time	Time at which the alert was triggered
Activity Details	Description of alert

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).

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

Edit Journal Monitor Rule

Use this task to edit a journal monitor rule.

To edit a Journal Monitor Rule

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

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.

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

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).

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

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

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

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).

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

Add Alert

Use this task to add a journal monitor alert.

To add alert

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

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

3) Complete the following fields.

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

> **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

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 Montior
- 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 Montior

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).

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

Field	Description
Rule ID	Unique Identifier assigned to message queue rule
Rule Name	Name assigned to the rule
Calendar	Name of the calendar that defines when the rule is applicable
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**: 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 - 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).

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

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

Field	Description
Rule ID	Unique ID assigned to the rule for which you are displaying criteria
Rule Name	Name assigned to the rule for which you are displaying criteria
Minimum Severity	The rule severity level that must be met to trigger a message (notification)
MSGID	Unique ID assigned to the message rule criteria
Message File	File in which the message rule resides
Message File Library	Library in which the message rule resides
Description	Description of rule
Message Omit or Select	Identifies whether the rule criteria 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	Reply sent to the recipient

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.

Field	Description
Alt Seq	The sequence in which alerts are sent **Note**: You might want to sequence your alerts so that more resource-heavy methods are executed last in the sequence.
Alert Type	Type of alert ***EMAIL** - Send an email alert to a specific user/group ***MSG** - Send a system message (message that appears when a user logs into the system) ***CMD** - Execute a command ***SYSLOG** - Send a notification to the system archive ***EMAILDIST** - Send an email alert to a specific user (legacy IBM method of sending email alerts) ***TGCENTRAL** - Send a notification to TGCentral
Alert Details	Recipient details
Message to Send	Text included in the notification sent to the designated recipient
Alert Criteria - #Events	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 **Freq** field.
Alert Criteria - Freq	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.

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.

Field	Description
Activity Type	Type of alert: ***EMAIL**- Email sent
Activity Status	Status of alert
Activity Date	Date on which the alert was triggered
Activity Time	Time at which the alert was triggered
Activity Details	Description of alert
Activity Details	Description of activity

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.

Field	Description
Rule ID	Enter a unique identifier for the message queue rule
Rule Name	Enter a name for the message queue rule
Calendar	Enter the name of the calendar that defines when the rule is applicable **Tip**: Enter ***NONE** if no calendar is applicable.

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

4) Press **Enter** twice.

Delete Message Queue Rule

Use this task to a delete 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** i nterface 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.

Field	Description
Message ID	Enter a unique ID for the message rule
Message File	Enter the file in which the message rule resides
Message File Library	Enter the library in which the message rule resides

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 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.

Tip: This feature is available only when variable fields (which appear with & placeholders) are present in the message description. See the following examples:

-- Message description with a single variable field: "Hardware failure on device **&1**"

-- Message description with multiple variable fields: "Controller **&1** on line **&2** failed"

-- Message description with no variable fields: "Error during PTF request"

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.

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.

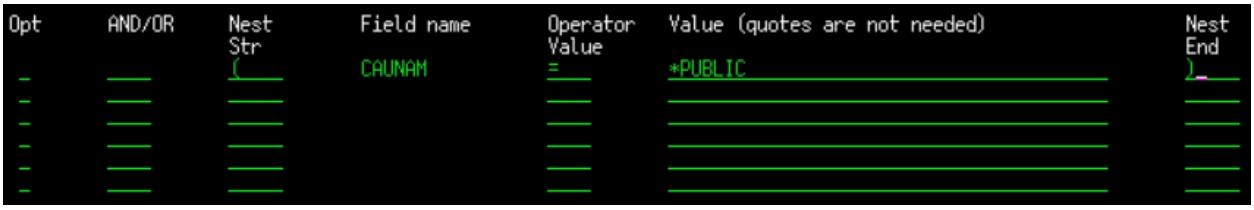
Tip: If the dialog contains no compare fields (blank), then this feature is not available for the selected message.

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 for filtering.

Tip: An SQL-like format is used to create report filters. For a list of supported operators, press the **F10** functi on 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 - 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).

Reply	Description
C	Cancel
G	Continue processing at *GETIN
D	Obtain RPG formatted dump
F	Obtain full formatted dump

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:

Field	Description
Monitor Messages Requiring Reply Only	Enter one of the following: ***NO** - Send notifications for all message in the queue ***YES** - Send notifications for only messages that required a reply **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:

Field	Description
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 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.

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

> **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 Header Changes Report

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

> **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 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.

Field	Description
Alert	Identifies whether an alert is sent: **Y** - Send an alert **N** - Do not send an alert **Note**: To see the SIEM log format in which the system sends alerts, refer to TGDetect Defaults
Code	Identifies the type of audit trail journal The following journal types are currently supported: **T** - Security journal **U** - User-defined journal
Type	Identifies the type of journal entry **Note**: Refer to the IBM Knowledge Center for a complete list of journal entry types and descriptions.
Descri ption	Description of journal entry
Field Filter	Identifies whether a field-level filter exists **Note**: Field-level filters all you to apply additional granularity to your monitor rules. **Y** - Field-level filter exists **N** - No field-level filter exists **Note**: To see the filter definition, refer to Manage SIEM Monitor Rule Criteria.
Field Select	Identifies whether the data from all fields or a subset of fields is sent **Note**: 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. **Y** - Send all fields **N** - Send a subset of fields **Note**: To see the subset of fields, refer to Manage SIEM Monitor Rule Criteria.
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 - 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).

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

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.

Field	Description
Seq	Sequence in which fields are sent to the SIEM
Field Name	Name of field
Field Description	Description of field

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).

3) Press **Enter**. The **Work with Rules - SIEM** 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 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 **W ork 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).

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

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

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

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.

Field	Description
Alert	Enter one of the options: **Y** - Send an alert to the SIEM for this type of journal entry **N** - Do not send an alert to the SIEM **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.

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

To edit the field filter

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

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.

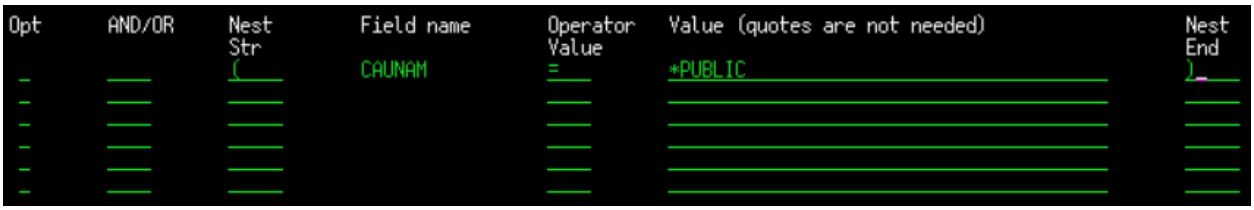
4) Place your cursor in the first available (blank) **Opt** column field and press the **F4** (Select Fields) function key on your keyboard. The list of field(s) from which you can apply a filter are displayed in a **Selection** dialog.

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.

> **Tip**: An SQL-like format is used to create report filters. For a list of supported operators, press the **F10** functi on 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 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

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 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.

> **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 to 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 TGDetect

Working with Monitors

Working with Monitor Rules

Manage Defaults

Groups

This section includes the following topic:

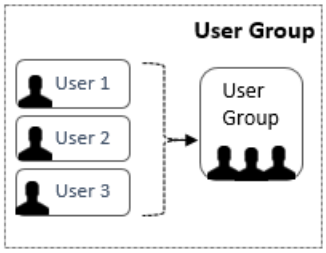
- Working with User Groups

See also

Getting Started

User Groups

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



This section includes the following topics:

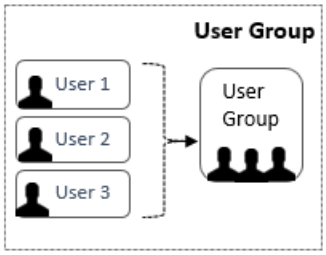
- Working with User Groups
- Display List of User Groups
- Display List of Users in a Group
- Manage User Groups
- Manage Users in a Group
- Run User Groups Report

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.

Product	Step
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.

Product	Step
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.

Product	Step
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 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.

Product	Step
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.

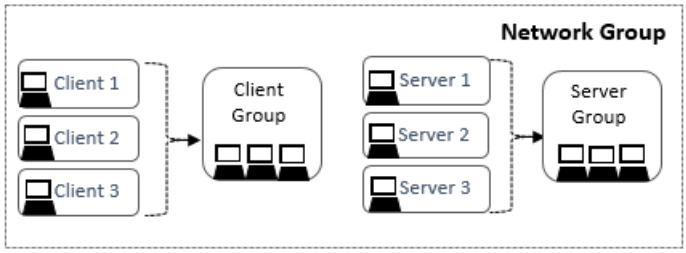
5) Press **Enter** twice.

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.

Product	Step
TGEncrypt	At the **Selection or command** prompt, enter **4** (Work with Groups).
TGSecure	At the **Selection or command** prompt, enter **31** (Work with Groups).

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 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.
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 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.

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.

Field	Description
Internet address	Enter the IP address of the SMTP server
Host name	Enter the host (website) URL for the SMTP server

Description	Enter a short description for the SMTP server

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

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.

Field	Description
Network user ID	Enter the user ID required to log into the network
Last name	Enter the user's last name
First name	Enter the user's first name
Middle name	Enter the user's middle name
Preferred name	Enter the user's preferred name

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

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.

Field	Description
Host name	Enter the name of the TCP/IP host
Domain name	Enter the web domain of the TCP/IP host

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 Distribution Attributes (CHGDSTA)** interface is displayed.

3) Complete the following fields.

Field	Description
Keep recipients	Enter one of the following options: ***ALL** - Keep all recipients ***BCC** - Keep recipients who are blind copied ***SAME** -Same as previous ***NONE** - Do not keep recipients
Use MSF for local	Enter one of the following options: ***YES** - Enable MSF (Message Switching Facility) ***NO** - Disable MSF ***SAME** - Same as previous
User ID	User ID of sender
Address	Email address of sender

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.

Field	Description

Autostart server	Enter one of the following options: ***YES** - Enable autostart ***NO** - Disable autostart ***SAME** - Use the value previously set (no change)
Clear e-mail on start-up	Enter one of the following options ***YES** - Enable clear e-mail on start-up ***NO** - Disable clear e-mail on start-up ***SAME** - Use the value previously set (no change)
E-mail directory type	Enter one of the following options: ***SMTP** - Simple Mail Transfer Protocol ***SMTPMSF** - Simple Mail Transfer Protocol (with Message Switching Facility) ***SDD** - System Distribution Directory ***SAME** - Use the value previously set (no change)
Retries by minute: Number of retries	Enter one of the following options: ***0-99** - Enter the number of access retries per minute. The max number of retries is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Retries by minute: Time interval	Enter one of the following options: ***0-99** - Enter the number of minutes to wait between retries. The max number of minutes is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Retries by day: Number of retries	Enter one of the following options: ***0-99** - Enter the number of access retries per day. The max number of retries is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Retries by day: Time interval	Enter one of the following options: ***0-99** - Enter the number of days to wait between retries. The max number of days is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Retries by hour: Number of retries	Enter one of the following options: ***0-99** - Enter the number of access retries per hour. The max number of retries is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Retries by hour: Time interval	Enter one of the following options: ***0-99** - Enter the number of hours to wait between retries. The max number of hours is 99. ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Coded character set identifier	Enter one of the following options: ***1-65533** - Enter the ASCII coded character set identifier (CCSI) used to map all single-byte character sets (SBCS) data on outgoing mail ***DFT** - Use system default value ***SAME** - Use the value previously set (no change)
Support ETRN for server	Enter one of the following options ***YES** - Enable support for ETRN (Extended Turn) servers ***NO** - Disable support for ETRN ***SAME** - Use system default value

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 **Severs**.

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.

Field	Description
Host Name	Enter the name of your mail server (e.g., SMTP.TrinityGuard.com)
User name	Enter the user name
User password	Enter the user's password
Confirm user password	Enter the user's password again for verification

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.

Field	Description
User profile	Enter the TG profile name of the user
SMTP mailbox alias	Enter the SMTP mailbox alias used to receive email notifications
Domain index	Enter the domain index. **Note**: A domain index determining which databases and/or files systems are to be included in the full text index.

> **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

> **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.

Field	Description
Syslog Provider Name	Enter the name of the Syslog provider
Syslog Provider Description	Enter a short description of the Syslog provider
Syslog IP Address	Enter the IP address at which the Syslog provider resides
Syslog Port	Enter the port you want to use to communicate to the Syslog provider
Syslog Protocol	Enter the protocol you want to use to communicate with the Syslog provider: **SSL** - Secure socket layer protocol **TCP** - Transmission control protocol **UDP** - User datagram protocol
Message Log Format	Enter the message log format you want to use to communicate with the Syslog provider: **CEF** - Common Event Format **GELF** - Graylog Extended Log Format **LEEF** - Log Event Extended Format **SYSLOG** - System Log
Syslog Facility	Enter the type of program logging the message
Syslog Severity	The severity of the message as defined by Syslog

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.

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

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 Bach 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

u

Collector ID	Collector Name	Collector Category	Platform
ACCESS_ESCAL_ACC_CONTROLS	Access Escalation Access Controls	Network	IBMi
ACCESS_ESCAL_DEFAULTS	Access Escalation Defaults	Network	IBMi
ACCESS_ESCAL_ENTITLEMENTS	Access Escalation Entitlements	Network	IBMi
ACCESS_ESCAL_FILE_EDITORS	Access Escalation File Editors	Network	IBMi
ACCESS_ESCALATION_USAGE	Access Escalation Usage	Network	IBMi
AUTH_USERS_VIA_AUTH_LISTS	Authorized Users through Authorization Lists	Resource	IBMi
AUTHORITY_COL_ALI	Authority Collection Report (*ALL)	Resources	IBMi
AUTHORITY_COL_IFS	Auth Collection For Objects IFS Report	Resources	IBMi
AUTHORITY_COL_OBJECT	Auth Collection For Objects Native Report	Resources	IBMi
AUTHORITY_COLLECTION	Authority Collection Data	Journal	IBMi
AUTHORITY_COMPLIANCE	Authority Compliance	Resource	IBMi
AUTHORITY_LIST	Authority List Data	System	IBMi
BLUEPRINT_3RD_PARTY_FILE	Blueprint 3rd Party Integration File	Profile	IBMi
BLUEPRINT_AUTH_SETTINGS_FILE	Blueprint Authority List Settings File	Profile	IBMi
BLUEPRINT_MASTER	Blueprint Master	Profile	IBMi
BLUEPRINT_NON_COMPLIANCE_USER	Blueprint Non-Compliance User Profiles	Profile	IBMi
BLUEPRINT_OBJECT_AUTH_FILE	Blueprint Object Authority File	Profile	IBMi
BLUEPRINT_PARAMETER_FILE	Blueprint Parameter File	Profile	IBMi
BLUEPRINT_PERMISSION_FILE	Blueprint Permission File	Profile	IBMi
CMD_SEC_COMMANDS	Commands Allowed/Rejected via Command Security	Resources	IBMi
CMD_SEC_CONF_SETTINGS	Command Security Config Settings	Resources	IBMi
CMD_SEC_PARAM_LEVEL	Command Security Paramater Level	Resources	IBMi
CMD_SEC_RULES	Command Security Config Settings	Resources	IBMi

CONTROLLER_ATTACHED_DEVICES	Command Security Paramater Level	Network	IBMi
CONTROLLER_DESCRIPTION_DATA	Controller Description Information	Network	IBMi
DATA_AREA_AUDITING	Audit data area changes	Network	IBMi
DATABASE ACCESS	Database File Access	N/A	IBMi
DATABASE_AUDITING	Monitor Database changes	Network	IBMi
DATABASE_CONTENT	Database Content	Configuration	IBMi
DATABASE_FIELD_ACTIVITY	Database Field Activity	Resources	IBMi
DATABASE_OPERATIONS	Database Operations	N/A	IBMi
DET_ACT_HISTORY	Detect Activity History	Network	IBMi
DET_DEFAULTS	Detect Defaults	Configuration	IBMi
DET_CMD_RULES	Command Monitor Rules	Configuration	IBMi
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration	IBMi
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration	IBMi
DET_JRNMON_RULES	Journal Monitor Rules	Configuration	IBMi
DET_MON_MASTER	Monitor Master	Configuration	IBMi
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration	IBMi
DET_MSQ_RULES	Message Queue Rules	Configuration	IBMi
DET_SEIM_PROVIDERS	SEIM Providers	Configuration	IBMi
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration	IBMi
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network	IBMi
DEVICE_DESCRIPTION_DATA	Device Description Information	Network	IBMi
DTBASE_OPERATIONS_JRN	Database Operations by Journal	N/A	IBMi
ENCRYPT_DATABASE_FIELD	Encryption Database Field Details	Resource	IBMi
ENCRYPT_DATABASE_FILE	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_FILTER	Encryption Database File Details	Resource	IBMi
ENCRYPT_DATABASE_RULES	Encryption Database Rule Details	Resource	IBMi
ENCRYPTION_DEFAULTS	Encryption Defaults	Resource	IBMi
EXIT_POINTS	Display Exit Point Data	Network	IBMi
FIELD_AUTHORITY	Display Field Level Authorities	Object	IBMi
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource	IBMi

IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource	IBMi
IFS_CONTENT	IFS Content	Configuration	IBMi
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource	IBMi
IFS_STATUS	Display status information about an IFS file	Resource	IBMi
INACTIVITY_DISCONNECTS	Inactivity Disconnections	Configuration	IBMi
INCOMING_TRANSACTIONS	Incoming Transactions	Network	IBMi
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network	IBMi
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network	IBMi
ISL_RULES	ISL Inclusion Exclusion Rules	Network	IBMi
JOB_ACTIVITY_DETAILS	Job Activity Details	Log	IBMi
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log	IBMi
JOB_DESCRIPTIONS	Job Description Data	Configuration	IBMi
JOURNAL_AD	Object Auditing Attribute Changes	Configuration	IBMi
JOURNAL_AF	Authority Failures	Profile	IBMi
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration	IBMi
JOURNAL_AU	EIM Attribute Changes	Configuration	IBMi
JOURNAL_AX	Row and Column Access Control	Resource	IBMi
JOURNAL_CA	Authorization List or Object Authority Changes	Profile	IBMi
JOURNAL_CD	Commands Executed	Resource	IBMi
JOURNAL_CO	Create Operations	Resource	IBMi
JOURNAL_CP	User Profile Changes	Configuration	IBMi
JOURNAL_CQ	Change Request Descriptor Changes	Configuration	IBMi
JOURNAL_CU	Cluster Operation	Network	IBMi
JOURNAL_CV	Connection Verification	Profile	IBMi
JOURNAL_CY	Cryptographic Configuration Changes	Configuration	IBMi
JOURNAL_DI	LDAP Operations	Resource	IBMi
JOURNAL_DO	Delete Operations	Resource	IBMi
JOURNAL_DS	Changes to Service Tools Profiles	Profile	IBMi
JOURNAL_EV	Environment Variable Changes	Profile	IBMi
JOURNAL_GR	Exit Point Maintenance Operations	Resource	IBMi

JOURNAL_GS	Socket Descriptor Details	Resource	IBMi
JOURNAL_IM	Intrusion Monitor Events	Network	IBMi
JOURNAL_IP	Inter-process Communication Events	Network	IBMi
JOURNAL_IR	Actions to IP Rules	Network	IBMi
JOURNAL_IS	Internet Security Management Events	Network	IBMi
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource	IBMi
JOURNAL_JS	Job Changes	Resource	IBMi
JOURNAL_KF	Key Ring File Changes	Configuration	IBMi
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource	IBMi
JOURNAL_M0	Db2 Mirror Setup Tools	Resource	IBMi
JOURNAL_M6	Db2 Mirror Communication Services	Resource	IBMi
JOURNAL_M7	Db2 Mirror Replication Services	Resource	IBMi
JOURNAL_M8	Db2 Mirror Product Services	Resource	IBMi
JOURNAL_M9	Db2 Mirror Replication State	Resource	IBMi
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration	IBMi
JOURNAL_NA	Network Attribute Changes	Profile	IBMi
JOURNAL_ND	Directory Search Violations	Resource	IBMi
JOURNAL_NE	APPN Endpoint Filter Violations	Network	IBMi
JOURNAL_O1	Single Optical Object Accesses	Resource	IBMi
JOURNAL_O2	Dual Optical Object Accesses	Resource	IBMi
JOURNAL_O3	Optical Volume Accesses	Resource	IBMi
JOURNAL_OM	Object Management Changes	Resource	IBMi
JOURNAL_OR	Objects Restored	Resource	IBMi
JOURNAL_OW	Object Ownership Changes	Resource	IBMi
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration	IBMi
JOURNAL_PF	PTF Operations	Resource	IBMi
JOURNAL_PG	Primary Group Changes	Resource	IBMi
JOURNAL_PO	Printer Output Changes	Resource	IBMi
JOURNAL_PS	Swap Profile Events	Configuration	IBMi
JOURNAL_PU	PTF Object Changes	Profile	IBMi
JOURNAL_PW	Invalid Sign-on Attempts	Profile	IBMi
JOURNAL_RA	Authority Changes to Restored Objects	Configuration	IBMi

JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration	IBMi
JOURNAL_RO	Ownership Changes for Restored Objects	Profile	IBMi
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration	IBMi
JOURNAL_RQ	Change Request Descriptors Restored	Resource	IBMi
JOURNAL_RU	Authority Restored for User Profiles	Profile	IBMi
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration	IBMi
JOURNAL_SD	System Directory Changes	Resource	IBMi
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration	IBMi
JOURNAL_SF	Spooled File Actions	Resource	IBMi
JOURNAL_SG	Asynchronous Signals Processed	Network	IBMi
JOURNAL_SK	Secure Socket Connections	Network	IBMi
JOURNAL_SM	Systems Management Changes	Configuration	IBMi
JOURNAL_SO	Server Security User Information Actions	Configuration	IBMi
JOURNAL_ST	Service Tools Actions	Configuration	IBMi
JOURNAL_SV	System Values Changes	Configuration	IBMi
JOURNAL_VA	Access Control List Changes	Configuration	IBMi
JOURNAL_VC	Connections Started, Ended, or Rejected	Network	IBMi
JOURNAL_VF	Close Operations on Server Files	Resource	IBMi
JOURNAL_VL	Exceeded Account Limit Events	Profile	IBMi
JOURNAL_VN	Network Log On and Off Events	Configuration	IBMi
JOURNAL_VO	Actions on Validation Lists	Resource	IBMi
JOURNAL_VP	Network Password Errors	Profile	IBMi
JOURNAL_VR	Network Resource Accesses	Resource	IBMi
JOURNAL_VS	Server Sessions Started or Ended	Network	IBMi
JOURNAL_VU	Network Profile Changes	Profile	IBMi
JOURNAL_VV	Service Status Change Events	Network	IBMi
JOURNAL_X0	Network Authentication Events	Network	IBMi
JOURNAL_X1	Identity Token Events	Profile	IBMi
JOURNAL_XD	Directory Server Extensions	Profile	IBMi
JOURNAL_YC	DLO Object Changes	Resource	IBMi
JOURNAL_YR	DLO Object Reads	Resource	IBMi
JOURNAL_ZC	Object Changes	Resource	IBMi

JOURNAL_ZR	Object Reads	Resource	IBMi
KEYSTORE_DATA	KeyStore	Configuration	IBMi
LIBRARY_STAT	Library Statistics	Resources	IBMi
LINE_DESCRIPTION_DATA	Line Description Information	Configuration	IBMi
MESSAGE_QUEUE	Message Queue Details	Configuration	IBMi
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration	IBMi
NETSERVER_CONFIG	NetServer Configuration	Network	IBMi
NETSERVER_SHARES	NetServer Shares	Network	IBMi
NETWORK_ATTRIBUTES	Network Attribute Information	Network	IBMi
NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network	IBMi
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network	IBMi
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network	IBMi
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network	IBMi
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network	IBMi
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network	IBMi
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network	IBMi
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network	IBMi
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes/Remote Exit Rule	Network	IBMi
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network	IBMi
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network	IBMi
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_DDM	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FILE	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_FTP_REXEC	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_PRINTER	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network	IBMi
NETWORK_TRANS_SIGNON	Remote Exit Rules	Network	IBMi
NETWORK_TRANS_TELNET	Remote Exit Rules	Network	IBMi

OBJECT_AUTHORITY	Display Object Authority	Resource	IBMi
OBJECT_DETAILS	Display Object Details	Resource	IBMi
OBJECT_STAT	Object/File Statistics	Resource	IBMi
OUTPUT_QUEUE	Output Queue Information	Configuration	IBMi
PRODUCT_INFO	Basic Information about a software product	Configuration	IBMi
PROFILE_COMPLIANCE	Profile Compliance Data	Profile	IBMi
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile	IBMi
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile	IBMi
PROGRAM_ADOPT	Programs that Adopt Authority	Resource	IBMi
PROGRAM_REFERENCE_DATA	Program Reference Data	Resource	IBMi
PTF_DATA	Program Temporary Fix Data	Configuration	IBMi
QHST_MSG_INFO	QHST History Log Information	Configuration	IBMi
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration	IBMi
QSYS2.DATA_QUEUE_ENTRIES	Data Queue Entries	Resource	IBMi
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration	IBMi
QSYS2.EXIT_POINT_INFO	Exit Point Information	Configuration	IBMi
QSYS2.EXIT_PROGRAM_INFO	Exit Program Information	Configuration	IBMi
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration	IBMi
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration	IBMi
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration	IBMi
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration	IBMi
QSYS2.JOURNALED_OBJECTS	Journal object information	Resource	IBMi
QSYS2.LICENSE_INFO	Products license information.	Configuration	IBMi
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration	IBMi
QSYS2.MEMORY_POOL	Memory pool details	Configuration	IBMi
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration	IBMi
QSYS2.MESSAGE_QUEUE_INFO	Message Queue	Configuration	IBMi

QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration	IBMi
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration	IBMi
QSYS2. OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration	IBMi
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration	IBMi
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration	IBMi
QSYS2. SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration	IBMi
QSYS2. SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration	IBMi
QSYS2. SERVER_SHARE_INFO	Server Share Information	Configuration	IBMi
QSYS2. SOFTWARE_PRODUCT	Server Software Product information	Configuration	IBMi
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration	IBMi
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration	IBMi
QSYS2.SYSDISKSTAT	Disk Information	Configuration	IBMi
QSYS2. SYSTEM_STATUS_INFO	Partition information	Configuration	IBMi
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration	IBMi
QSYS2.USER_INFO	User Profile Information	Configuration	IBMi
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration	IBMi
REMOTE_TRAN_SUMMARY_ BY_SERVER	Remote Summary Server	Network	IBMi
REMOTE_TRAN_SUMMARY_ BY_USER	Remote Summary User	Network	IBMi
RSC_MGR_COMPLIANCE_DA TA	Resource Manager Authority Out of compliance data	Network	IBMi
RSC_MGR_CONFIG	Resource Manager Configuration	Network	IBMi
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network	IBMi
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network	IBMi
SENSITIVE_DATABASE_CON TENT	Sensitive Database Content	Profile	IBMi
SERVICE_TOOL_SECURITY_ ATTR	Service Tool Security Attributes	Profile	IBMi
SERVICE_TOOL_USERS	Service Tool User Data	Profile	IBMi

SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network	IBMi
SOCKET_SUMMARY_BY_USER	Socket Summary by User	Network	IBMi
SOCKET_TRAN_RULES	Socket Rules	Network	IBMi
SOCKET_TRANSACTIONS	Socket Transactions	Network	IBMi
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration	IBMi
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration	IBMi
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration	IBMi
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration	IBMi
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration	IBMi
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration	IBMi
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration	IBMi
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration	IBMi
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration	IBMi
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration	IBMi
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration	IBMi
SYS_VAL_CONFIG	System Value Configuration	Configuration	IBMi
SYS_VAL_DEFAULT	System Value Default	Configuration	IBMi
SYS_VAL_VALID	System Value Default	Configuration	IBMi
SYSCOLAUTH	Privileges Granted on a Column	Configuration	IBMi
SYSCONTROLS	Permission or Column Mask Defined	Configuration	IBMi
SYSCONTROLSDEP	Dependencies of Row Permissions and Column Masks	Configuration	IBMi
SYSCONTROLSDEP	Privileges Granted on a Row	Configuration	IBMi
SYSFIELDS	Columns with Field Procedures	Configuration	IBMi
SYSPACKAGEAUTH	Privileges Granted on a Package	Configuration	IBMi
SYSPROGRAMSTAT	Program, Service Program, and Module with SQL Statements	Configuration	IBMi
SYSROUTINEAUTH	Privileges Granted on a Routine	Configuration	IBMi
SYSSCHEMAAUTH	Privileges Granted on a Schema	Configuration	IBMi
SYSSEQUENCEAUTH	Privileges Granted on a Sequence	Configuration	IBMi
SYSTABAUTH	Privileges Granted on a Table or View	Configuration	IBMi

SYSTABLESTAT	Table Statistics Include all Partitions and Members	Configuration	IBMi
SYSTEM_VALUES	Display System Value Data	System	IBMi
SYSTOOLS. GROUP_PTF_CURRENCY	PTF Groups Installed per IBM Recommendations	Configuration	IBMi
SYSTOOLS. GROUP_PTF_DETAILS	PTFs within PTF Groups Installed per IBM Recommendations	Configuration	IBMi
SYSUDTAUTH	Privileges Granted on a Type	Configuration	IBMi
SYSVARIABLEAUTH	Privileges Granted on a Global Variable	Configuration	IBMi
SYSXSROBJECTAUTH	Privileges Granted on an XML Schema	Configuration	IBMi
TGMOBJINF	Object Information	Resource	IBMi
TG_NETWORK_GROUPS	TG Network Groups	Network	IBMi
TG_OBJECT_GROUPS	TG Object Groups	Network	IBMi
TG_OPERATION_GROUPS	TG Operation Groups	Network	IBMi
TG_USER_GROUPS	TG User Groups	Network	IBMi
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile	IBMi
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile	IBMi
USER_PROFILE_ACTIVITY	User Profile Activity	Profile	IBMi
USER_PROFILE_ARCHIVE	User Profile Archive	Profile	IBMi
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile	IBMi
USER_PROFILES	Display User Profile Data	Profile	IBMi

APPENDIX - TGDetect Built-in History Log (QHST) Rules

The History Log Monitor contains the following pre-defined rules:

Rule ID	Rule Name	Create notifications about the following:
Damage_Objects	Damage Objects	Detection of error or damage to object(s) The following are the out-of-the box message IDs available for **Damage_Objects**: • CPFAFA0 - Errors detected on MSF internal message index • CPFAFA1 - Errors detected on MSF internal message queue • CPFA09F - Object damaged. Object is &1 • CPFBB83 - Internal cluster object damaged • CPF0C19 - Damage occurred on object &1 in library &2 **Note**: This is not an exhaustive list of message IDs–just a sample. Access the History Log Monitor to view the complete list.
Hardware_Failures	Hardware failures and Critical conditions	Detection of hardware failures or critical conditions The following are the out-of-the box message IDs available for **Hardware_Failures**: • CPA3576 - Error during PTF request. Press Help before replying • CPA5201 - Hardware failure on device &3 • CPA578C - Controller &24 online &23 failed. Probable insufficient resources • CPFAD93 - APPC failure. Failure code is &3 • CPP8988 - A critical system hardware problem has occurred. Critical Message Handler has been run
Invalid_Signon	Invalid Signon Attempts	Detection of invalid sign-on attempts The following are the out-of-the box message IDs available for **Invalid_Signon**: • CPF1393 - User profile &2 has been disabled • CPF1397 - Subsystem &1 varied off work station &3 for user &8 • CPF2234 - Password from device &1 not correct for user &2

Licensing	Licensing Issues	Detection of licensing expirations, limitations, etc. The following are examples of the out-of-the box message IDs available for **Licensing**: • 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.
Multiple_Receivers	Multiple Receivers for journal per X hours	Detection of multiple receivers The following are the out-of-the box message IDs available for **Multiple_Receivers**: • CPC7011 - Journal receiver &1 created in library &2 **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.
Qsecofr_Signon	Monitor QSECOFR Signon	Detection of signon by a high-profile (QSECOFR) The following are the out-of-the box message IDs available for **Qsecofr_Signon**: • 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
QAUDCTL_Changes	Monitor QAUDCTL Changes	Detection of change to changes to system values The following are the out-of-the box message IDs available for **QAUDCTL_Changes**: • CPF180F - System value &1 changed

Storage_Issues	Storage Issues	Detection of storage limit capacity issues The following are the out-of-the box message IDs available for **Storage_Issues**: • CPFA08F - User profile storage limit exceeded • CPFA80A - Data queue &1 is full • CPFB515 - Not enough storage in machine pool • CPFB569 - Main storage allocation failure occurred • CPF090A - Temporary storage threshold reached • CPF950A - Storage limit exceeded for data queue &1 in &2 • CPI1468 - System job tables nearing capacity
Subsystem_Messages	Subsystem Messages	Detection of subsystem failures (i.e., cannot open, start, or find) The following are examples of out-of-the box message IDs available for **Subsystem_Messages**: • CPF1011 - Start subsystem failed for SBSD &1 in library &2 • CPF117A - Subsystem &1 cannot start autostart job &2 • CPF1171 - Subsystem &1 cannot find file &2 in library &3 • CPF1172 - Subsystem &1 cannot open file &2 in library &3 **Note**: This is not an exhaustive list of message IDs–just a sample. Access the History Log Monitor to view the complete list.
System_Events	System events and subsystem activity	Detection of system and system activities that impact security The following are examples of out-of-the box message IDs available for **System_Events**: • CPFAD10 - An error was detected in the exit program &1 in library &2 • CPF0849 - Space addressing violation • CPF0927 - Subsystem &1 ended • CPF0934 - IPL completed • CPF1103 - Subsystem &1 started **Note**: This is not an exhaustive list of message IDs–just a sample. Access the History Log Monitor to view the complete list.

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