NetIQ Security Solutions for IBM i
TGDetect 2.1
User Guide
Revised August 2019

Legal Notice

Table of Contents

What's New in Version 2.1

This release includes the following:

- 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

1. Introduction

1.1. TGDetect Overview

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.

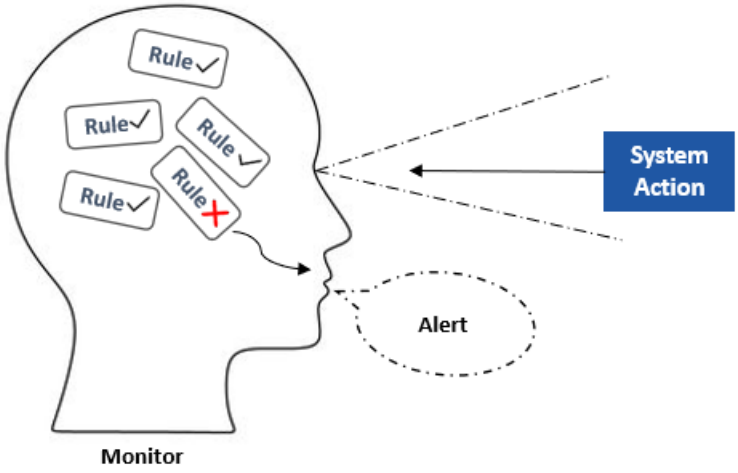
See also

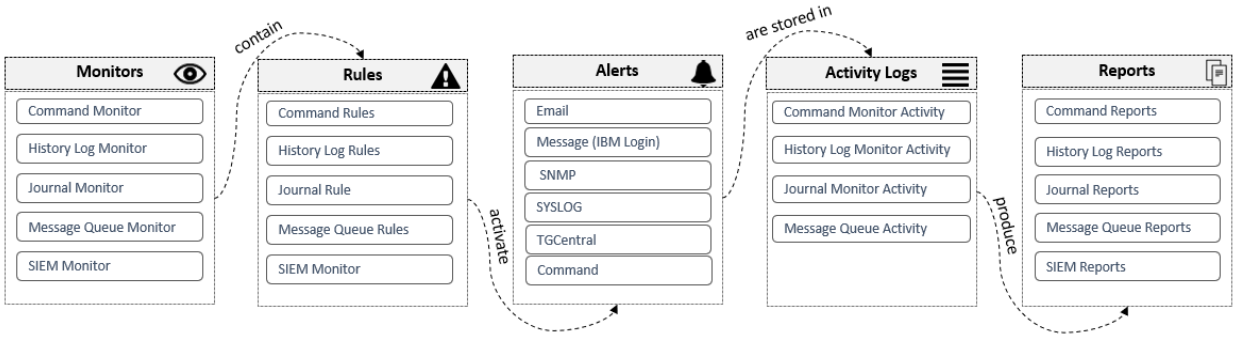
Features

Use TGDetect

1.2. 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

TGDetect Overview

Features

2. Getting Started

2.1. 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**.

Note: The **TG - Main Menu** interface is displayed.

4) At the **Selection or command** prompt, enter **3** (TGDetect).

Note: The **TGDetect Main** menu is displayed.

See also

Features

Use TGDetect

2.2. Getting Started Using TGDetect

This topic discusses the following:

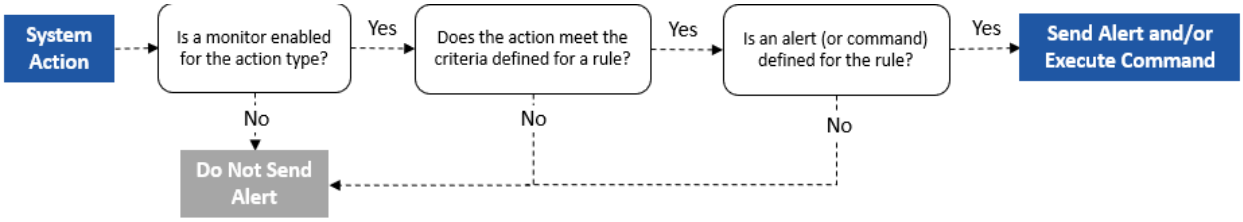
- Actions
- Process Flow
- Implementation Tasks

2.2.1. 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

2.2.2. Process Flow



2.2.3. 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 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.
Step 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.
Step 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.
Step 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.
Step 5	**Create Alerts** To define the designated recipient for a notification, you must create alerts. See Working with Monitor Alerts for additional information.
Step 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.
Step 7	**Run Reports** Run report to monitor activity and track changes. See Working with Monitor Reports for additional information.

See also

Log Into TGDetect

Features

3. Defaults

3.1. Working with 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.).

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.

Note: The **Main** menu appears.

2) At the **Selection or command** prompt, enter **11** (TGDetect Defaults).
3) Press **Enter**.

Note: The **Work with TGDetect Default Setting** interface is displayed.

See also

Log into TGDetect

Use TGDetect

Manage TGDetect Defaults

Run TGDetect Default Reports

3.2. Manage TGDetect Defaults

Use this task to do the following:

- Add collection interval defaults
- Add SIEM defaults
- Add auditing defaults
- Start subsystem
- Stop subsystem

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

3.2.1. Access the TGDetect Default Settings Interface

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

T**o 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**.

Note: The **TGDetect Default Setting** interface is displayed.

3.2.2. Add Collection Interval Defaults

Use this task to add timing for the collection of system activities for specific monitors 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 minutes) how often to check the history log monitor for alerts that required sending
Message Queue	Enter (in minutes) how often to check the message queue monitor for alerts that required sending
Real-time Journal	Enter (in minutes) how often to check the journal monitor for alerts that required sending

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

3) Press **Enter.**

3.2.3. 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
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

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

3) Press **Enter.**

3.2.4. 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.**

3.2.5. 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 monitor (other than disabling all the individual monitors) is to stop the subsystem.

To add audit defaults

1) Access the **TGDetect Default Setting** interface.
2) Press **F22** (Start subsystem) on your keyboard.

3.2.6. 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 monitor (other than disabling all the individual monitors) 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

3.3. Run Default Setting Reports

Use this task to generate the following reports:

- Default settings
- Default setting changes

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

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

3.3.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

3.3.2. Run Default Settings Report

Use this report to display the list of defaults 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

3.3.3. 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 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with TGDetect Defaults

Working with Reports

4. Monitors

4.1. 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 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.

Note: The **Main** menu appears.

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

Note: The **Work with Monitors** interface is displayed.

See also

Log into TGDetect

Use TGDetect

Working with Monitor Rules

4.2. Display Monitors

Use this task to do the following with monitors:

- Display list
- Move to position in list
- Sort list

4.2.1. 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**.

Note: 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)
Description	Description of the monitor
Protect	Whether monitor is internal (built-in): **Note**: Internal monitors are shipped with the product and cannot be deleted compare to custom message queue monitors which can be deleted. **Y** - Internal (cannot be deleted) **N** - Custom (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

4.2.2. 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.

4.2.3. 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**.

Note: 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

4.3. Manage Monitors

Use this task to do the following:

- Add a monitor
- Delete a monitor
- Start a monitor
- End a monitor
- Work with monitor rules

To manage monitors, access from 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**.

Note: The **Work with Monitors** interface is displayed.

4.3.1. 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 message specific to the user.

To add a monitor

1) Access the **Work with Monitors** interface.
2) Press the **F6** (Add Monitor) function key.

Note: The **Work with Monitor - Add record**.

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 message 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.

4.3.2. 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.

4.3.3. Start Monitor

Use this task to enable a monitor. Once enabled the monitor will begin collecting information, evaluating activities to established monitoring rules, and sending alerts (notifications).

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

To start monitoring

1) Access the **Work with Monitor** interface.
2) In the **OPT** column for the desired monitor, enter **1** (Start Monitor).
3) Press **Enter** twice.

Note: Monitors that you disable (end) should appear with a status of ***ACTIVE**.

4.3.4. 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.

Note: Monitors that you disable (end) should appear with a status of ***INACTIVE**.

4.3.5. Work with Monitor Rules

See Working with Monitor Rules

4.3.6. Work with Activity

See the following topics:

- Display Command Monitor Activity Log
- Display History Log Activity Log
- Run Monitor Master Reports

4.4. Run Monitor Master Reports

Use this task to generate the following reports:

- Monitor master report
- All activity report

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

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

4.4.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

4.4.2. 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**.

Note: The status of the report is displayed at the bottom of the screen.

4.4.3. Run All Activity Report

Use this report to display the list 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**.

Note: 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**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Monitors

Working with Reports

4.5. Command Monitor

4.5.1. Working with Command Monitor

This section describes working with Command Monitor (CMD):

- 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

In order 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**.

Note: The **Work with Monitors** interface is displayed.

See also

Log into TGDetect

Use TGDetect

4.5.2. Display Command Monitors Rules

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

- Display list
- Filter list
- Sort list

4.5.2.1. 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**.

Note: 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

4.5.2.2. 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.

4.5.2.3. 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 around text (e.g., *report*) 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**.

Note: 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

4.5.3. Display Command Monitors Rule Criteria

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

- Display list
- Filter list
- Sort list

4.5.3.1. 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4) In the **OPT** column for the desired command monitor rule, enter **10** (Rule Criteria).

Note: 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

4.5.3.2. 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 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.

4.5.3.3. 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 around text (e.g., *report*) 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**.

Note: 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

4.5.4. 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).

T**o display 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4) In the **Opt** column for the desired rule, enter **20** (Alerts).

Note: 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

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 Command Monitor Rules

Manage Command Monitor Alerts

4.5.5. 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 associates 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4) In the **Opt** column for the desired history log rule, enter **30** (Work with Activity).

Note: 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

4.5.6. Manage Command Monitor Rules

Use this task to do the following:

- Add command monitor rule
- Delete command monitor rule
- Edit command monitor rule
- Edit command monitor rule criteria
- Edit command monitor alerts

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

4.5.6.1. Access Work with Rules - CMDMON interface

T**o 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4.5.6.2. 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.

Note: 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.

4.5.6.3. 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.

4.5.6.4. 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.

4.5.6.5. Edit Command Monitor Rule Criteria

See Manage Command Monitor Rule Criteria.

4.5.6.6. Edit Command Monitor Alerts

See Manage Command Monitor Alerts.

See also

Working with Command Monitor Rules

Display Command Monitor Rules

4.5.7. Manage Command Monitor Rule Criteria

Use this task to do the following:

- Add rule criteria
- Delete rule criteria
- Edit rule criteria

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

4.5.7.1. Access Work with Rule Criteria - CMD interface

T**o 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4) In the **OPT** column for the desired command monitor rule, enter **10** (Rule Criteria).

Note: The **Work with Rule Criteria - CMD** interface is displayed.

4.5.7.2. 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.

Note: 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.

4.5.7.3. 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.

4.5.7.4. 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.

See also

Working with Command Monitor Rules

Display Command Monitor Rule Criteria

4.5.8. Manage Command Monitor Alerts

Use this task to do the following:

- Add alert
- Delete alert
- Edit alert

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

4.5.8.1. Access Work with Alert - CMDMON Interface

T**o 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**.

Note: The **Work with Rules - CMDMON** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alert).

Note: The **Work with Alert - CMDMON** interface is displayed.

4.5.8.2. 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.

Note: 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 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.

4.5.8.3. 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.

4.5.8.4. 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.

See also

Working with Command Monitor Rules

Display Command Monitor Alerts

4.5.9. Run Command Monitor Reports

Use this task to generate the following reports:

- Command monitor activity report
- Command monitor alert report
- Command monitor alert change report
- Command monitor rule report
- Command monitor rule change report

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

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

4.5.9.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

4.5.9.2. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.5.9.3. 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**.

Note: The status of the report is displayed at the bottom of the screen.

4.5.9.4. Run Command Monitor Alert Change Report

Use this report to display the list 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**.

Note: The status of the report is displayed at the bottom of the screen.

4.5.9.5. 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**.

Note: The status of the report is displayed at the bottom of the screen.

4.5.9.6. 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**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Command Monitor Rules

Working with Monitor Reports

4.6. History Log Monitor

4.6.1. Working with History Log Monitor

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

- 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

In order 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**.

Note: The **Work with Monitors** interface is display.

See also

Log into TGDetect

Use TGDetect

4.6.2. Display History Log Rules

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

- Display list
- Filter list
- Sort list

4.6.2.1. 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**.

Note: The **Work with Rules** interface is displayed.

Field	Description
Rule ID	Unique Identifier assigned to history log 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

4.6.2.2. 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.

4.6.2.3. 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 around text (e.g., *report*) 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**.

Note: 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

4.6.3. Display History Log Rule Criteria

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

- Display list
- Filter list
- Sort list

4.6.3.1. 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**.

Note: The **Work with Rules - QSYS/QHST** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **10** (Rule Criteria).

Note: 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

Field	Description
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

4.6.3.2. 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.

4.6.3.3. 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 around text (e.g., *report*) 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**.

Note: 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

4.6.4. 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alerts).

Note: 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

4.6.5. 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **30** (Work with Activity).

Note: 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

4.6.6. Manage History Log Rules

Use this task to do the following:

- Add history log rule
- Delete history log rule
- Edit history log rule
- Edit history log rule criteria
- Edit History log alerts

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

4.6.6.1. 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**.

Note: The **Work with Rules - QSYS/QHST** interface is displayed.

4.6.6.2. 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.

Note: 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.

4.6.6.3. 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.

4.6.6.4. 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.

4.6.6.5. Edit History Log Rule Criteria

See Manage History Log Rule Criteria.

4.6.6.6. Edit History Log Alerts

See Manage History Log Alerts.

See also

Working with History Log Rules

Display History Log Rules

4.6.7. Manage History Log Rule Criteria

Use this task to do the following:

- Add rule criteria
- Delete rule criteria
- Edit rule criteria
- Change minimum severity
- Compare field
- Add replies

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

4.6.7.1. Access Work with Rule Criteria - QSYS/QHST interface

T**o 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **10** (Rule Criteria).

Note: The **Work with Rule Criteria - QSYS/QHST** interface is displayed.

4.6.7.2. 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.

Note: 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.

4.6.7.3. 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.

4.6.7.4. 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.

4.6.7.5. Change Minimum Severity

Use this task when you want to limit message notification by severity level. By default, the severity minimum is set to zero, which includes all severity levels.
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.

Note: The **Work with Rule Criteria - Change Severity** interface is displayed

3) Complete the following fields.

Field	Description
Minimum Severity	Enter the minimum severity level require: **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**.

4.6.7.6. 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.

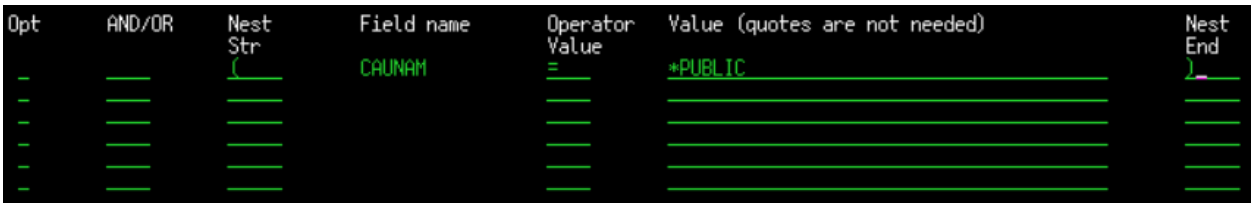
Tip: If the dialog contains no compare fields (blank), then this feature is not available for the selected message.

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 the 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**.

4.6.7.7. Add Replies

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**.

See also

Working with History Log Rules

Display History Log Rule Criteria

4.6.8. Manage History Log Alerts

Use this task to do the following:

- Add alert
- Delete alert
- Edit alert

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

4.6.8.1. Access Work with Alert - QSYS/QHST interface

T**o 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alert).

Note: The **Work with Alert - QSYS/QHST** interface is displayed.

4.6.8.2. 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.

Note: 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 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.

Field	Description
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.

4.6.8.3. 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.

4.6.8.4. 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.

See also

Working with History Log Rules

Display History Log Alerts

4.6.9. Run History Log Reports

Use this task to generate the following reports:

- History log activity report

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

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

4.6.9.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

4.6.9.2. 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**.

Note: 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with History Log Rules

Working with Monitor Reports

4.7. Journal Monitor

4.7.1. Working with Journal Monitor

This section describes working with Journal Monitor (JRN):

- 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

In order 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**.

Note: The **Work with Monitors** interface is displayed.

See also

Log into TGDetect

Use TGDetect

4.7.2. Display Journal Monitor Rules

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

- Display list
- Filter list
- Sort list

4.7.2.1. 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**.

Note: 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 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.
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

4.7.2.2. 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.

4.7.2.3. 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 around text (e.g., *report*) 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**.

Note: 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

4.7.3. Display Journal Monitor Rule Criteria

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

- Display Field Filter

4.7.3.1. 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 **4** (Journal Monitor Rules).
3) Press **Enter**.

Note: 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 exists 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).

Note: 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

4.7.4. 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 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**.

Note: 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).

Note: 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

4.7.5. 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 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**.

Note: 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).

Note: 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

4.7.6. Manage Journal Monitor Rules

Use this task to do the following:

- Edit journal monitor rule
- Edit journal monitor rule criteria
- Edit journal monitor alerts

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

4.7.6.1. 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**.

Note: The **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface is displayed.

4.7.6.2. 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).

Note: 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 desire calendar. **Tip**:

4.7.6.3. Edit Journal Monitor Rule Criteria

See Manage Journal Monitor Rule Criteria

4.7.6.4. Edit Journal Monitor Alerts

See Manage Journal Monitor Alerts

See also

Working with Journal Monitor

Display Journal Monitor Rules

4.7.7. Manage Journal Monitor Rule Criteria

Use this task to do the following:

- Edit field filter

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

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

T**o 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**.

Note: The **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface is displayed.

4.7.7.2. 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**.

Note: 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.

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

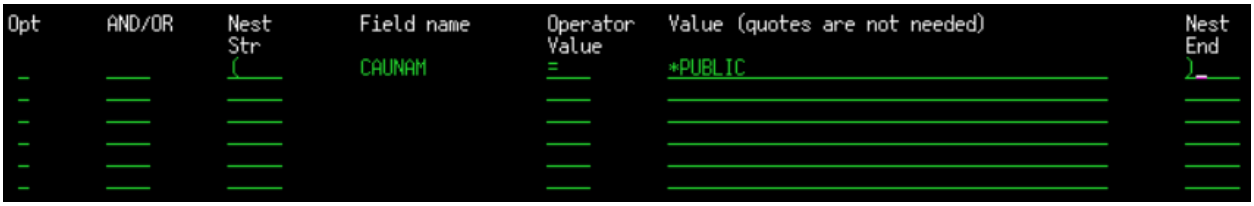
5) Enter **1** in the **Sel** column for the field(s) you want to use for filtering.

6) Press **Enter**.

Note: 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

4.7.8. Manage Journal Monitor Alerts

Use this task to do the following:

- Add alert
- Delete alert
- Edit alert

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

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

T**o 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**.

Note: The **Work with Rules - Realtime Journal QSYS/QAUDJRN** interface is displayed.

4.7.8.2. 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.

Note: 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

Field	Description
	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.

4.7.8.3. 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.

4.7.8.4. 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

4.7.9. Run Journal Monitor Reports

Use this task to generate the following reports:

- Journal monitor activity report
- Journal monitor alert report
- Journal monitor rule report
- Journal monitor rules details change report
- Journal monitor rule for SIEM report
- Journal monitor rule for SIEM change report

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

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

4.7.9.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

4.7.9.2. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.7.9.3. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.7.9.4. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.7.9.5. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.7.9.6. Run Journal Monitor Rules for SIEM Report

See Run SIEM Reports

4.7.9.7. 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

4.8. Message Queue Monitor

4.8.1. Working with Message Queue

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

- 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

In order 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**.

Note: The **Work with Monitors** interface is displayed.

See also

Log into TGDetect

Use TGDetect

4.8.2. Display Message Queue Rules

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

- Display list
- Filter list
- Sort list

4.8.2.1. 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**.

Note: 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

4.8.2.2. 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.

4.8.2.3. 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 around text (e.g., *report*) 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 Rules

4.8.3. Display Message Queue Rule Criteria

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

- Display list
- Filter list
- Sort list

4.8.3.1. 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**.

Note: The **Work with Rules - MSGQ** interface is displayed.

4) In the **OPT** column for the desired message queue rule, enter **10** (Rule Criteria).

Note: 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

Field	Description
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

4.8.3.2. 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.

4.8.3.3. 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 around text (e.g., *report*) 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

4.8.4. 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alerts).

Note: 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

4.8.5. 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 list of message queue notifications

1) Access the TGDetect **Main** menu.
2) At the **Selection or command** prompt, enter **3** (Message Queue Rules).
3) Press **Enter**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **30** (Work with Activity).

Note: 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

4.8.6. Manage Message Queue Rules

Use this task to do the following:

- Add message queue rule
- Delete message queue rule
- Edit message queue rule
- Edit journal monitor rule criteria
- Edit journal monitor alerts

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

4.8.6.1. 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**.

Note: The **Work with Rules - MSGQ** interface is displayed.

4.8.6.2. 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.

Note: 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.

4.8.6.3. 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.

4.8.6.4. 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.

4.8.6.5. Edit Message Queue Rule Criteria

See Manage Message Queue Rule Criteria.

4.8.6.6. Edit Message Queue Alerts

See Manage Message Queue Alerts.

See also

Working with Message Queue Rules

Display Message Queue Rules

4.8.7. Manage Message Queue Rule Criteria

Use this task to do the following:

- Add rule criteria
- Delete rule criteria
- Edit rule criteria
- Change minimum severity
- Compare fields
- Add replies

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

4.8.7.1. Access the Work with Rule Criteria - MSGQ interface

T**o 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**.

Note: The **Work with Rules - MSGQ** interface is displayed.

4) In the **OPT** column for the desired message queue rule, enter **10** (Rule Criteria).

Note: The **Work with Rule Criteria - MSGQ** interface is displayed.

4.8.7.2. Add Rule Criteria

Use this task to add message queue rule criteria.

To add rule criteria

1) Access the **Work with Rule Criteria - MSGQ** interface.
2) Press the **F6** (Add) function key.

Note: 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.

4.8.7.3. Delete Rule Criteria

Use this task to delete a message queue rule criteria.

To delete rule criteria

1) Access the **Work with Rule Criteria - 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 rule criteria.
5) Press **Enter** twice.

4.8.7.4. Edit Rule Criteria

Use this task to edit the message queue rule criteria

To edit rule criteria

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

4.8.7.5. Change Minimum Severity

Use this task when you want to limit message notification by severity level. By default, the severity minimum is set to zero, which includes all severity levels.
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.

Note: The **Work with Rule Criteria - Change Severity** interface is displayed

3) Complete the following fields.

Field	Description
Minimum Severity	Enter the minimum severity level require: **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**.

4.8.7.6. 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 - MSGQ** 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.

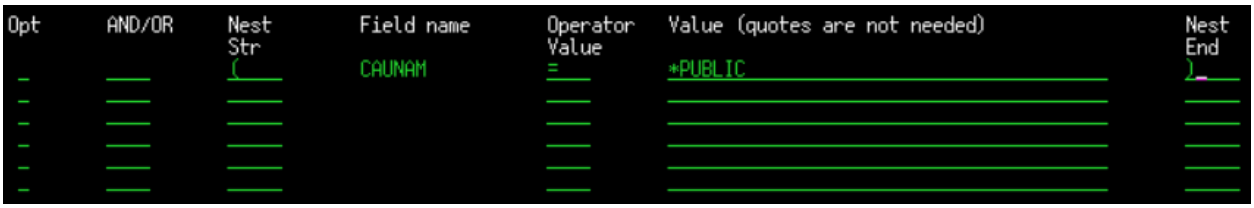
Tip: If the dialog contains no compare fields (blank), then this feature is not available for the selected message.

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 the 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**.

4.8.7.7. Add Replies

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.
5) Press **Enter**.

See also

Working with Message Queue Rules

Display Message Queue Rule Criteria

4.8.8. Manage Message Queue Alerts

Use this task to do the following:

- Add alert
- Delete alert
- Edit alert

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

4.8.8.1. Access Work with Alert - MSGQ interface.

T**o 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**.

Note: The **Work with Rules** interface is displayed.

4) In the **OPT** column for the desired history log rule, enter **20** (Alert).

Note: The **Work with Alert - MSGQ** interface is displayed.

4.8.8.2. 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.

Note: 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.

4.8.8.3. 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.

4.8.8.4. 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

4.8.9. Run Message Queue Reports

Use this task to generate the following reports:

- Message queue activity report
- Message queue alert report
- Message queue alert change report
- Message queue rule report
- Message queue rules header changes report
- Message queue rules details changes report

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

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

4.8.9.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

4.8.9.2. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.8.9.3. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.8.9.4. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.8.9.5. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.8.9.6. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

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

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

4.8.9.7. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with Message Queue Rules

Working with Monitor Reports

4.9. SIEM Monitor

4.9.1. Working with SIEM Monitor

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

- Display SIEM Monitor Rules

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

In order 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**.

Note: The **Work with Monitors** interface is displayed.

See also

Log into TGDetect

Use TGDetect

4.9.2. Display SIEM Monitor Rules

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

- Display list
- Filter list
- Sort list

4.9.2.1. 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**.

Note: 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.
Description	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

4.9.2.2. 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.

4.9.2.3. 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 around text (e.g., *report*) 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**.

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

See also

Working with SIEM Monitor Rules

Manage SIEM Monitor Rules

Manage SIEM Monitor Rule Criteria

4.9.3. 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 filter

4.9.3.1. 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**.

Note: 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 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).

Note: 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

4.9.3.2. 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**.

Note: 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).

Note: 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

4.9.4. Manage SIEM Monitor Rules

Use this task to do the following:

- Edit SIEM monitor rule
- Edit SIEM monitor rule criteria

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

4.9.4.1. 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**.

Note: The **Work with Rules - SIEM Journal** interface is displayed.

4.9.4.2. 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).

Note: 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.

4.9.4.3. Edit SIEM Monitor Rule Criteria

See Manage SIEM Monitor Rule Criteria.

See also

Working with SIEM Monitor Rules

Display SIEM Monitor Rules

Manage Defaults

4.9.5. Manage SIEM Monitor Rule Criteria

Use this task to do the following:

- Edit field list
- Edit field filter

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

4.9.5.1. 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**.

Note: The **Work with Rules - SIEM Journal** interface is displayed.

4.9.5.2. 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**.

Note: 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**.

Note: 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**.

4.9.5.3. 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**.

Note: 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.

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

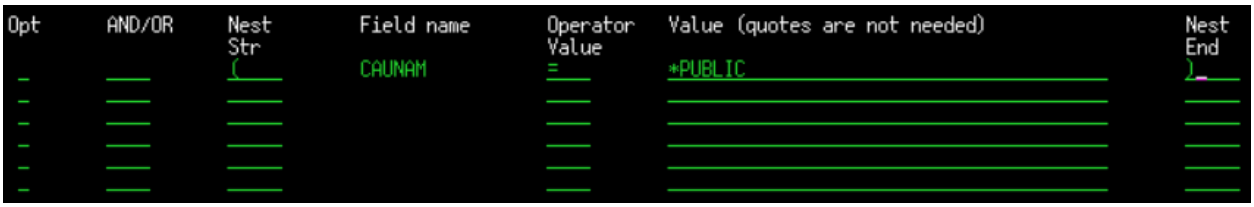
5) Enter **1** in the **Sel** column for the field(s) you want to use for filtering.

6) Press **Enter**.

Note: 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 SIEM Monitor Rules

Manage SIEM Monitor Rules

4.9.6. Run SIEM Reports

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

- SIEM activity report
- SIEM provider report
- SIEM provider change report
- Journal monitor rules for SIEM report
- Journal monitor rules for SIEM change report

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

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

4.9.6.1. 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**.

Note: The **TGDetect Reports** interface is displayed.

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

4.9.6.2. Run SIEM Activity Report

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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.9.6.3. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.9.6.4. 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.9.6.5. Run Journal Monitor Rules for SIEM Report

Use this report to display 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.

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**.

Note: The status of the report is displayed at the bottom of the screen.

4.9.6.6. 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.

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**.

Note: 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

5. Rules

5.1. 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

In order to work with rules, you must access the **Work with Rules** interface.

To access the Work with Rules interface

1) Log into to TGDetect.

Note: The **Main** menu appears.

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

Note: The **Work with Monitor** interface is displayed.

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

Note: The **Work with Rules** interface is displayed.

See also

Log into TGDetect

Use TGDetect

Working with Monitors

Working with Monitor Reports

6. Activity Log

6.1. 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

Use TGDetect

Working with Monitors

Working with Monitor Rules

7. Reports

7.1. Working with Monitor Reports

This section describes working with monitor reports.

Note: 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 a list of reports available.

In order to work with rules, you must access the **TGDetect Reports** interface.

To access the TGDetect Reports interface

1) Log into to TGDetect.

Note: The **Main** menu appears.

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

Note: The **TGDetect Reports** interface is displayed.

See also

Log into TGDetect

Use TGDetect

Working with Monitors

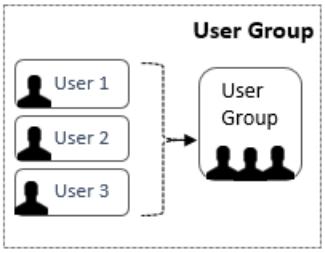
Working with Monitor Rules

Manage Defaults

8. Groups

8.1. Working with User Groups

This section describes what you need to know about user groups.



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

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

To access 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**.

Note: The **Work with User Groups** interface is displayed.

See also

Display List of User Groups

Display List of Users

Manage User Groups

Manage Users

Run User Groups Report

8.2. Display List of User Groups

Use this task to do the following with user groups:

- Display the list of user groups

- Sort the list of user groups
- Move to a specific location within the list of user groups
- Filter the list user groups

8.2.1. Display List

Use this task to display the list of user groups.

To display the list of user groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

To display the list of user groups

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **10** (Work with User Groups).
3) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

8.2.2. 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.

8.2.3. 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.

8.2.4. 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 around text (e.g., *report*) 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**.

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

See also

Working with User Groups

8.3. Manage User Groups

Use this task to do the following with user groups:

- Add user groups
- Edit user groups
- Copy user group
- Delete user groups

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

To access the Work with User Groups interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.

Note: The **Work with User Groups** interface is displayed.

8.3.1. 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.

8.3.2. 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.

8.3.3. 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.

8.3.4. 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

8.4. Display List of Users in a Group

Use this task to do the following with user groups:

- Display the list of users within a group
- Sort the list of users within a group
- Move to a specific location within the list of users

8.4.1. Display List

Use this task to display the list of users assigned to a user group.

To display the list of users assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column, enter **10** (Work with Users).
7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

To display the list of users assigned to a group

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **10** (Work with User Groups).
3) Press **Enter**.
4) In the **OPT** column, enter **10** (Work with Users).
5) Press **Enter**.

Note: The **Work with Users** interface is displayed.

8.4.2. 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.

8.4.3. 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

8.5. Manage Users Within a Group

Use this task to do the following with user groups:

- Add users
- Edit users
- Delete users

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

To access the Work with Users interface

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Groups).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **1** (Work with User Groups).
5) Press **Enter**.
6) In the **OPT** column of the user group you want to manage, enter **10** (Work with Users).
7) Press **Enter**.

Note: The **Work with Users** interface is displayed.

8.5.1. 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**.

8.5.2. 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.

8.5.3. 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

8.6. Run User Groups Report

Use this task to generate reports that display the following for user groups.

- User group configuration details
- User group configuration changes

8.6.1. Run User Group Configuration Report

Use this task to display user group configuration details.

To run User Group Configuration Report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **3** (Configuration Reports).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (User Groups Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

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.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

8.6.2. Run User Group Configuration Changes Report

Use this task to display the list of configuration changes made to user groups.

Tip: You must enable auditing to produce change reports. See Enable Access Escalation Change Auditing for additional information.

To run User Group Configuration Changes Report

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **1** (Network Security).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Network Reports).
5) Press **Enter**.
6) At the **Selection or command** prompt, enter **4** (Configuration Changes).
7) Press **Enter**.
8) At the **Selection or command** prompt, enter **4** (User Groups Changes Report).
9) Press **Enter**.
10) Modify the run criteria as necessary.

Note: The criteria allow you to limit the data returned in the report when you generate it.

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.

11) Enter the desired output format in the **Report output type** field.
12) Press **Enter**.

Note: The status of the report is displayed at the bottom of the screen.

See also

Working with User Groups

9. Email/Syslog Setup

9.1. 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.

- Working with Email Setup
- Working with Syslog Setup

In order 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.

Note: The **Main** menu appears.

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

Note: The **Email/Syslog Configuration** interface is displayed.

See also

Log into TGDetect

Use TGDetect

9.2. Email Setup

9.2.1. Alerts

9.2.1.1. Working with Monitor Alerts

This section describes working with monitor 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

Use TGDetect

Working with Monitors

Working with Monitor Rules

9.2.2. Working with Email Setup

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

- Manage email setup

In order to work with email setup, you must access the **Email Setup** interface.

To access the Email Setup interface

1) Log into to TGDetect.

Note: The **Main** menu appears.

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

Note: The **Email/Syslog Configuration** interface is displayed.

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

Note: The **Email Setup** interface is displayed.

See also

Log into TGDetect

Use TGDetect

Working with Email/Syslog Setup

9.2.3. Manage Email Setup

Use this task to do the following:

Note: The tasks must be complete 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

To manage email setup, access from the **Email Setup** interface.

9.2.3.1. Access the Email Setup Interface

To access the Email Setup interface

1) Log into to TGDetect.

Note: The **Main** menu appears.

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

Note: The **Email/Syslog Configuration** interface is displayed.

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

Note: The **Email Setup** interface is displayed.

9.2.3.2. (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).

Note: 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.

9.2.3.3. (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).

Note: 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.

9.2.3.4. (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).

Note: 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.

9.2.3.5. (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).

Note: 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.

9.2.3.6. (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).

Note: 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)

Field	Description
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.

9.2.3.7. (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.

Note: 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**.

Note: 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.

Note: 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**.

9.2.3.8. (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.

9.2.3.9. (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).

Note: 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

9.3. Syslog Setup

9.3.1. Working with Syslog Setup

This section describes tasks you need to perform to setup Syslog alerts.

- Manage Syslog setup

In order 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**.

Note: 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

Use TGDetect

Working with Email/Syslog Setup

9.3.2. Manage Syslog Setup

Use this task to do the following:

- Display list of Syslog providers
- Add Syslog provider
- Edit Syslog provider

To manage the Syslog setup, access from the **Email/Syslog Configuration** interface.

9.3.2.1. 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**.

Note: The **Email/Syslog Configuration** interface is displayed.

9.3.2.2. 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 definition that you can edit as necessary.

To display the list of Syslog providers

1) Access the **Email/Syslog Configuration** interface.
2) At the **Selection or command** prompt, enter **2** (Syslog Configuration).
3) Press **Enter**.

Note: 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.

9.3.2.3. Add Syslog Provider

Use this task to add a Syslog provider

To add a Syslog provider

1) Access the **Email/Syslog Configuration** interface.
2) At the **Selection or command** prompt, enter **2** (Syslog Configuration).
3) Press **Enter**.

Note: 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	Severity of message as defined by Syslog

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

6) Press **Enter**.

9.3.2.4. 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**.

Note: 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**.

See also

Working with Syslog Setup

10. Save and Restore Configuration

10.1. Save/Restore TG Configuration

The **Save/Restore TG Configuration** 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

Note: A saved file store the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules

See also

Manager Configuration

10.2. Manage Configuration

Use the **Save/Restore TG Configuration** feature to do the following:

- Save the configuration definition of a specific agent
- Restore the configuration of an agent
- Copy the configuration of an agent

10.2.1. Save Configuration

Use this task to save the configuration of a specific agent for later restoration or to transfer the configuration to another agent.

Caution: If you have TGDetect installed and licensed, end the TGDetect subsystem before attempting to save a configuration. If you are running TGDetect subsystems at the time you attempt to save your configuration, you will receive an error message.

To save the configuration

1) Access the **IBM i Main** menu.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Save/Restore Configuration).

Note: The **Save/Restore TG Configuration (TGSAVRST)** interface is displayed.

5) Complete the following fields:

Field	Description
Product component	Identify the configuration component(s) you want to save. The options available are as follows: ***ALL** - Save all components ***RPT** - Save reports, report cards settings, and audit configuration ***JAM** - Save JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Save network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Save AEM (Access Escalation Manager) entitlements, groups, calendars, editors, defaults, and access control ***ISL** - Save ISL (Inactive Session Lockdown) defaults, rules, options ***RSC** - Save Resource Manager defaults, schemas, collections configuration ***PRF** - Save Profile Manager defaults, blueprints, user exclusions, password rules, etc. ***DET** - Save TGDetect defaults **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***SAVE** to create a configuration file--which creates an archive of the current configuration settings-- for the selected product components.

6) Click **Enter**.
7) Complete the following fields:

Field	Description
Save file	Enter the name you want to assign the save file or enter ***DEFAULT** to use the default name (i.e., TGSAVCFG).
Library	Enter the name of the library in which to store the save file or enter ***CURLIB** to store the file in the current library.
Clear Save File	Whether to override the save file (if it exists) ***YES** - Override the existing file ***NO** - Do not override an existing save file **Tip**: If this setting is set to ***NO** and you attempt to create a save file with the same name as an existing save file, you will receive an error message. You have two options if you receive an error message: --If you want to override the existing save file, change the option to ***YES** --If you do not want to override the existing save file, leave the option set to ***NO** and change the name of the save file you want to create, thereby, avoiding the override of the existing save file
Target Release	Enter the release for which you want to save a configuration: ***CURRENT** - Save the configuration for the currently installed operating system (OS) ***PRV** - Save the configuration to work with the previous OS **Tip**: Use the **F4** keyboard function to see the complete list of available OS versions. **Note**: The max number of previous OS versions for which you can create a save file are two.

Field	Description
	For example, if you are running V7R3M0 currently, you could do the following: -- Enter ***CURRENT** to create a save file compatible with V7R3M0 (currently installed OS in this example) -- Enter ***PRV** to create a save file compatible with V7R2M0 (one version older than current OS in this example) -- Manually enter **V7R1M0** (two versions older than current OS version in this example). If you attempt to create a save file for a version greater than two previous OS releases, you will receive an error message.
Run interactively	Whether to run interactively or add to batch: ***YES** - Run the report immediately ***NO** - Add the report to a batch job to be run when most efficient for the system

8) Click **Enter**.

Note: If a saved configuration file already exists with the defined name in the preferred library, you will receive an information message. You can choose to cancel the save (C) or replace (G) the file.

10.2.2. Restore Configuration

Use this task to restore the configuration of your agent to a previous state using an existing save file.

Caution: If you have TGDetect installed and licensed, end the TGDetect subsystem before attempting to restore a configuration. If you are running TGDetect subsystems at the time you attempt to restore your configuration, you will receive an error message.

To restore the configuration

1) Access the **IBM i Main** menu.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**.
4) At the **Selection or command** prompt, enter **20** (Save/Restore Configuration).

Note: The **Save/Restore TG Configuration (TGSAVRST)** interface is displayed.

5) Complete the following fields:

Field	Description
Product component	Identify the configuration component(s) you want to restore. Your options are as follows: ***ALL** - Restore all components ***RPT** - Restore reports, report cards settings, and audit configuration ***JAM** - Restore JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Restore network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Restore AEM (Access Escalation Manager) entitlements, groups, calendars, editors, defaults, and access control ***ISL** - Restore ISL (Inactive Session Lockdown) defaults, rules, options ***RSC** - Restore Resource Manager defaults, schemas, collections configuration ***PRF** - Restore Profile Manager defaults, blueprints, user exclusions, password rules, etc.

Field	Description
	***DET** - Restore TGDetect defaults **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***RESTORE** to use an existing save file to restore the configuration to a previous state.

6) Click **Enter**.
7) Complete the following fields:

Field	Description
Save file	Enter the name of the save file you want to use to restore the configuration or enter ***DEFAULT** to use the default name (i.e., TGSAVCFG).
Library	Enter the name of the library in which the save file is stored.
Run Interactively	Enter one of the following options: ***YES** - Run the restore job immediately ***NO** - Add the restore job to the queue

8) Click **Enter**.

10.2.3. Copy Configuration

Use this task to copy the configuration of one agent to another agent.

To copy the configuration

1) Follow the instructions to save a configuration instance.
2) Use whatever method (e.g., FTP) you are most comfortable with to transfer the save file (e.g., TGSAVCFG).

Tip: You must transfer the save file manually onto each server on which you want to restore a specific configuration.

3) Follow the instruction to restore a configuration instance.

See also

Save/Restore TG Configuration

11. Troubleshooting

11.1. Fix Files

TGFix is a tool introduced in version 2.0 that allows you to install fixes via the TG menu quickly and easily. The feature also includes verification features that ensure the fix is installed properly.

See also

Save Fix to Agent Server

Manage Fixes

Display List of Fixes

11.2. Save Fix to Agent Server

Use this task to save the TGFix file to the agent server. You must FTP the fix file to the server before you can apply it.

To save the fix to the agent server

1) Open a DOS or command window.
2) Type the following command, substituting the name of the iSeries server for [system-name].

   FTP [system-name]

Alternatively: You can use the iSeries IP (internet address) instead of the system name.

3) Use the iSeries command **GO TCPADM** to find the address.
4) Select option **7**.
5) Select option **1**.
6) Type a user ID at the FTP prompt and press **Enter**.
7) Type the password at the FTP prompt and press **Enter**.
8) Type the following command to create the TGFIX library if it does not exist on your iSeries server:

   quote rcmd crtlib TGFIX

9) Type the following command to create the save file if it does not exist on your iSeries server:

   quote rcmd crtsavf TGFIX/TGF018001

10) Type the following command to transfer the file using binary image mode:

    binary

11) Type the following command to identify the path, where [path] is the folder where you saved the file in Step 2:

    lcd [path]

12) Type the following command to transfer the file from the PC to the iSeries:

    put TGF018001.svf TGFIX/TGF018001

13) Type the following command to end FTP:

quit

14) Type the following command to close the DOS window:

exit

See also

Fix Files

Apply Fix

Display List of Fixes

11.3. Manage Fixes

Use this task to do the following:

- Apply fix
- Remove fix

Note: If you are working with a newly release version, there might not be fixes necessary/available. You will be notified as fixes become available.

11.3.1. Apply Fix

Use this task to apply a fix.

Tip: The fix file must be saved on the agent server before attempting to apply it.

To apply a fix

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **TGFIX**.
3) Press the **F4** (Prompt) function key.

Note: The **TG Fix Manager (TGFIX)** interface is displayed.

4) Complete the following fields:

Field	Description
Fix ID	Enter the fix ID, which should be provided to you in the following format: (TGFVVVXXX) Where: **TGF** = TG Fix **VVV** = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Fix action to perform	Enter ***APY**

5) Press **Enter**.

Note: The TGFix program performs validations before applying the fix (e.g., is the fix file present on the agent server, has the fix already been applied, etc.)

11.3.2. Remove Fix

Use this talk to remove a fix.

To remove a fix

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **TGFIX**.
3) Press the F4 (Prompt) function key on your keyboard.

Note: The **TG Fix Manager (TGFIX)** interface is displayed.

4) Complete the following fields:

Field	Description
Fix ID	Enter the fix ID, which should be provided to you in the following format: (TGFVVVXXX) Where: **TGF** = TG Fix **VVV** = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Fix action to perform	Enter ***RMV**

5) Press **Enter**.

See also

Fix Files

Save Fix to Agent Server

Display List of Fixes

11.4. Display List of Fixes

Use this task to display the list of fixes applied to the agent.

To display the list of fixes

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **80** (Licensing Status).
3) Press **Enter**.
4) Press the **F6** (Add Key) function key on your keyboard.
5) Enter the license key.
6) Press **Enter**.

Field	Description
Fix ID	The Fix ID is based on the following nomenclature: **TGFVVVFFF**

Field	Description
	Where: **TGF** = TG Fix **VVV** = Three-digit version number. **FFF** = Three-digit numeric number (assigned sequentially) to each fix **Note**: For example, TGF020001 would be the 1st (001) TG fix for version 2.0 (020)
Applied Date	Date on which the fix was applied to the system
Apply User	User who applied the fix

See also

Fix Files

Manage Fixes