



NetIQ Security Solutions for IBM i

TGDetect 2.0

Report Reference Guide

Revised January 2019

Legal Notice

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

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

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

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

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

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

Copyright © 2019 Trinity Guard LLC. All rights reserved.

Table of Contents

TABLE OF CONTENTS.....	III
1. INTRODUCTION.....	5
1.1. REPORT CATEGORIES	5
2. ACTIVITY HISTORY REPORTS	7
2.1. ACTIVITY HISTORY REPORTS.....	7
2.2. HISTORY LOG ACTIVITY	7
2.3. MESSAGE QUEUE ACTIVITY.....	8
2.4. COMMAND MONITOR ACTIVITY.....	10
2.5. JOURNAL MONITOR ACTIVITY.....	11
2.6. SEIM ACTIVITY	13
3. CONFIGURATION REPORTS.....	15
3.1. CONFIGURATION REPORTS.....	15
3.2. MONITOR MASTER	15
3.3. SEIM PROVIDERS	16
3.4. MESSAGE QUEUE RULES	17
3.5. COMMAND MONITOR RULES	19
3.6. MESSAGE QUEUE AND COMMAND ALERTS	20
3.7. JOURNAL MONITOR RULES	21
3.8. JOURNAL MONITOR ALERTS.....	22
3.9. JOURNAL MONITOR RULES FOR SEIM	24

1. Introduction

This reference guide provides information about each build-it report in TGDetect.

Please refer to the TGDetect User Guide for detailed information and concepts on how to use TGDetect.

1.1. Report Categories

There are three categories of TGDetect reports:

- [Activity History Reports](#)
- [Configuration Reports](#)
- [Change Reports](#)

2. Activity History Reports

2.1. Activity History Reports

This section contains descriptions for the following reports:

- All Activity
- [History Log Activity](#)
- [Message Queue Activity](#)
- [Command Monitor Activity](#)
- [Journal Monitor Activity](#)
- [SEIM Activity](#)

2.2. History Log Activity

This report displays a list of history log activities.

The report is based on the following collector:

- Det_Act_History

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
- 5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

- 6) At the **Selection or command** prompt, enter **2** (History Log Activity).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: *QHST - History log monitor

Column	Description
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

[Activity History Reports](#)

2.3. Message Queue Activity

This report displays a list of message queue activities.

The report is based on the following collector:

- Det_Act_History

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
- 5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

- 6) At the **Selection or command** prompt, enter **3** (Message Queue Activity).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: *MSGQ - Message queue monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)

Column	Description
User Name	Name user who performed system activity

See Also

[Activity History Reports](#)

2.4. Command Monitor Activity

This report displays a list of command monitor activities.

The report is based on the following collector:

- Det_Act_History

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
- 5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

- 6) At the **Selection or command** prompt, enter **4** (Command Monitor Activity).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: *CMD - Command monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place

Column	Description
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

[Activity History Reports](#)

2.5. Journal Monitor Activity

This report displays a list of journal monitor activities.

The report is based on the following collector:

- Det_Act_History

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
- 5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

- 6) At the **Selection or command** prompt, enter **5** (Journal Monitor Activity).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: *JRN - Journal monitor
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

[Activity History Reports](#)

2.6. SEIM Activity

This report displays a list of SEIM activities.

The report is based on the following collector:

- Det_Act_History

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **1** (Activity History Reports).
- 5) Press **Enter**.

Note: The **Activity History Reports** interface is displayed.

- 6) At the **Selection or command** prompt, enter **6** (SEIM Activity).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: *SEIM - Journal archival monitor (used for batch jobs)
Rule ID	ID assigned to monitor rule
Event Timestamp	Time at which the monitor identified the system activity
Activity Type	Type of a system activity
Activity Status	Status of the system activity
Activity Timestamp	Time at which the system activity took place
Activity Details	Description of the system activity
Syslog IP Address	IP address of the Syslog (system log) server
Syslog Port	Port used to communicate to the Syslog
Syslog Protocol	Protocol used to communicate to the Syslog
Syslog Facility	Type of program logging the message

Column	Description
Syslog Severity	Severity of message as defined by Syslog
Job Number	Number assigned to the job
Job Name	Name assigned to the job
Message Severity	Severity of message
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Program Name	Name of the program
System Name	IBM agent (system)
User Name	Name user who performed system activity

See Also

[Activity History Reports](#)

3. Configuration Reports

3.1. Configuration Reports

This section contains descriptions for the following reports:

- Default Settings
- [Monitor Master](#)
- [SEIM Providers](#)
- [Message Queue Rules](#)
- [Command Monitor Rules](#)
- [Message Queue and Command Alerts](#)
- [Journal Monitor Rules](#)
- [Journal Monitor Alerts](#)
- [Journal Monitor Rules and SEIM](#)

3.2. Monitor Master

This report displays the complete list of monitors (built-in and custom).

The report is based on the following collector:

- Det_Mon_Master

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **2** (Monitor Master).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored

Column	Description
Monitor Type	Type of monitor: *CMD - Command monitor *JRN - Journal monitor *MSGQ - Message queue monitor *QHST - History log monitor *SEIM - Journal archival monitor (used for batch jobs)
Monitor Description	Description of monitor
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)
Last Processed Status	Time at which data was last collected
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Monitor Job Name	Name assigned to the job
Monitor Job User	User who performed the job
Monitor Job Number	Number assigned to the job

See Also

[Configuration Reports](#)

3.3. SEIM Providers

This report displays the list of SEIM providers.

The report is based on the following collector:

- Det_SEIM_Providers

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **3** (SEIM Providers).

- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Syslog Provider Name	Name of the Syslog provider
Syslog Provider Description	Description of Syslog provider
Syslog IP Address	IP address for Syslog server
Syslog Port	Port used to communicate with Syslog
Syslog Protocol	Protocol used to communicate with Syslog
Message Log Format	Format in which messages are communicated to Syslog
Syslog Facility	Type of program logging the message
Syslog Severity	Severity of message

See Also

[Configuration Reports](#)

3.4. Message Queue Rules

This report displays the list of message queue monitor rules.

The report is based on the following collector:

- Det_Msq_Rules

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **4** (Message Queue Rules).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Rule ID	ID assigned to the rule
Rule Name	Name assigned to the rule
Calendar Name	Calendar that defines when the rule is valid
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Message Queue	Name of the message queue
Message Queue Library	Library in which the message queue resides
Message ID	ID assigned to the message
Message File	Name of the message file object
Message File Library	Library in which message file object resides
Filter Sequence	Sequence in which rules are applied (in increments of 10)
Before Nesting Lvl	Character used to begin a nested filter (open parenthesis)
And OR	Boolean operator used in rule definition
Field Name	Field to be analyzed using the rule
Condition	Condition used in the rule definition
Value	Field value used in the rule definition
After Nesting Lvl	Character used to end a nested filter (close parenthesis)
Message Field Compare	Identifies whether a field-level filter exists Note: field-level filters allow you to apply additional granularity to your monitor rules. Y - Field-level filter exists N - No field-level filter exists
Message Omit or Select	Identifies whether the rule criteria is used for selecting or omitting: S - Rule criteria used to identify messages to include (trigger alerts) O - 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.

See Also

[Configuration Reports](#)

3.5. Command Monitor Rules

This report displays the list of command monitor rules.

The report is based on the following collector:

- Det_Cmd_Rules

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **5** (Command Monitor Rules).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Rule ID	ID assigned to the rule
Rule Name	Name assigned to the rule
Calendar Name	Calendar that defines when the rule is valid Note: * NONE appears if no calendar is applicable.
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year
Command Name	Name of the command to be monitor
Command Library	Name of the library to be monitor
Command User	Name of the user to be monitor

See Also

[Configuration Reports](#)

3.6. Message Queue and Command Alerts

This report displays the list of message queue and command alerts.

The report is based on the following collector:

- Det_Msq_Cmd_Alr

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **6** (Message Queue and Command Alerts).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Note: The fields populated are dependent on the alert type.

Column	Description
Monitor Name	Name of the monitor
Monitor Library	Library to be monitored
Monitor Type	Type of monitor: * CMD - Command monitor * MSGQ - Message queue monitor * QHST - History log monitor
Rule Name	Name assigned to the monitor rule
Alert Sequence	Sequence in which alerts are to be sent
Alert Type	Type of alert to be sent: * 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

Column	Description
Forward Message Queue	Name of the message queue
Forward Message Queue Library	Library in which message queue resides
Email Address	Email address of the designated recipient
Email Message	Email message to be sent to the designated recipient
Command to Execute	Command to be executed (as defined by monitor rule definition)
SNMP Trap ID	SMTP Trap object identifier
SEIM Name	Name of the SEIM
Alert Criteria Volume	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.
Alert Criteria Frequency	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 a notification only if the 10 failed login attempts occurred within a 1-hour period.
Alert Criteria Measurement	Enter the frequency unit: MIN - Minutes HR - Hours DAYS - Days
Alert Criteria First Processed Time	Time at which first alert was sent
Alert Criteria Alerts in Period	Number of alerts sent

See Also

[Configuration Reports](#)

3.7. Journal Monitor Rules

This report displays the list of journal monitor rules.

The report is based on the following collector:

- Det_JrnMon_Rules

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **7** (Journal Monitor Rules).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Column	Description
Journal Name	Name of the journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Calendar Name	Calendar that defines when the rule is valid Note: *NONE appears if no calendar is applicable.
Journal Alert	Identifies whether an alert has been defined
Journal Filter	Identifies whether a filter has been defined
Alerts Processed Today	Number of alerts triggered today
Alerts Processed This Month	Number of alerts triggered this month
Alerts Processed This Year	Number of alerts triggered this year

See Also

[Configuration Reports](#)

3.8. Journal Monitor Alerts

This report displays the list of journal monitor alerts.

The report is based on the following collector:

- Det_JrnMon_Alerts

To run this report

- 1) Access the TGDetect main menu.

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

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **8** (Journal Monitor Alerts).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

- 9) Press **Enter**.

Report Column Description

Note: The fields populated are dependent on the alert type.

Column	Description
Journal Name	Name of the journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Alert Sequence	Sequence in which alerts are to be sent
Alert Type	Type of alert to be sent: *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
Forward Message Queue	Name of the message queue
Forward Message Queue Library	Library in which message queue resides
Email Address	Email address of the designated recipient
Email Message	Email message to be sent to the designated recipient
Command to Execute	Command to be executed (as defined by monitor rule definition)
SNMP Trap ID	SMTP Trap object identifier

Column	Description
SEIM Name	Name of the SEIM
Alert Criteria Volume	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.
Alert Criteria Frequency	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 a notification only if the 10 failed login attempts occurred within a 1-hour period.
Alert Criteria Measurement	Enter the frequency unit: MIN - Minutes HR - Hours DAYS - Days
Alert Criteria First Processed Time	Time at which first alert was sent
Alert Criteria Alerts in Period	Number of alerts sent

See Also

[Configuration Reports](#)

3.9. Journal Monitor Rules for SEIM

This report displays the list of journal monitor rules for SEIM.

The report is based on the following collector:

- Det_Jrn_SEIM_Rules

To run this report

- 1) Access the TGDetect main menu.
- 2) At the **Selection or command** prompt, enter **20** (Reporting).
- 3) Press **Enter**.

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

- 4) At the **Selection or command** prompt, enter **2** (Configuration Reports).
- 5) Press **Enter**.

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

- 6) At the **Selection or command** prompt, enter **9** (Journal Monitor Rules for SEIM).
- 7) Press **Enter**.
- 8) Modify the run criteria as necessary.

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

9) Press **Enter**.

Report Column Description

Column	Description
Journal Name	Name of the journal to be monitored
Journal Library	Library in which journal resides
Journal Code	Code that identifies the type of journal entry
Journal Type	Code that identifies the type of journal
Filter Sequence	Sequence in which filters (rules) are to be applied
Before Nesting Lvl	Character used to begin a nested filter (open parenthesis)
And OR	Boolean operator used in rule definition
Field Name	Field to be analyzed using the rule
Condition	Condition used in the rule definition
Value	Field value used in the rule definition
After Nesting Lvl	Character used to end a nested filter (close parenthesis)
Field Name	Name of the field to be communicated with SEIM
Field Sequence	Sequence in which fields should be communicated to SEIM
Secondary Field?	** This field is reserved for future use **

See Also

[Configuration Reports](#)