NetIQ Security Solutions for IBM i
TGAudit 2.2
User Guide
Revised April 2020

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© 2020 Trinity Guard LLC. All rights reserved.

1. What's New . . . 5
2. TGAudit Introduction . . . 7
2.1 Benefits . . . 8
2.2 Features . . . 9
3. Setup . . . 10
3.1 Configure TGAudit . . . 11
3.2 Log Into TGAudit . . . 12
3.3 Set Up Alert Defaults . . . 13
3.4 Set Up Data Area Journaling . . . 14
3.5 Set Up Database Journaling . . . 15
3.6 Set Up Integrated File System Auditing . . . 16
3.7 Set Up Job Scheduler . . . 17
3.8 Set Up Object Auditing . . . 18
3.9 Set Up Range of Journal Receivers for Reports . . . 19
3.10 Set Up System Auditing . . . 20
3.11 Clean Up Journal Receivers . . . 22
3.12 Clean Up Report Data . . . 24
4. Getting Started . . . 25
4.1 Use TGAudit . . . 26
5. Reports . . . 27
5.1 Built-in Reports . . . 28
5.1.1 Working with Reports . . . 29
5.1.2 Display List of Reports . . . 30
5.1.3 Run Reports . . . 32
5.2 Custom Reports . . . 35
5.2.1 Working with Custom Reports . . . 36
5.2.2 Create Custom Reports . . . 37
5.2.3 Manage Custom Reports . . . 41
5.2.4 Run Custom Reports . . . 44
5.3 Authority Collection Reports . . . 45
5.3.1 Working with Authority Collection Reports . . . 46
5.4 Data Level Reports . . . 47
5.4.1 Working with Data Level Reports . . . 48
5.5 Security and Configuration Reports . . . 49
5.5.1 Working with Security and Configuration Reports . . . 50
6. Report Cards . . . 51
6.1 Built-in Report Cards . . . 52
6.1.1 Working with Report Cards . . . 53
6.1.2 Display List of Report Cards . . . 54
6.1.3 Run Report Cards . . . 56
6.2 Custom Report Cards . . . 57
6.2.1 Working with Custom Report Cards . . . 58
6.2.2 Create Custom Report Card . . . 59
6.2.3 Manage Custom Report Cards . . . 61
6.2.4 Run Custom Report Card . . . 63
6.3 Regulation Report Cards . . . 64
6.3.1 Working with Regulation Report Cards . . . 65
6.3.2 Run Australia Standard Report Card . . . 66
6.3.3 Run COBIT 5 Report Card . . . 67
6.3.4 Run CSA Report Card . . . 68
6.3.5 Run FFIEC Report Card . . . 69
6.3.6 Run FISMA Report Card . . . 70
6.3.7 Run GAPP Report Card . . . 72
6.3.8 Run GLBA Report Card . . . 73
6.3.9 Run HIPAA Report Card . . . 75
6.3.10 Run IRS Publication 1075 . . . 77
6.3.11 Run ISO 27001 Report Card . . . 78
6.3.12 Run ITIL KPI Report Card . . . 80
6.3.13 Run NERC Report Card . . . 81
6.3.14 Run Nevada Standard Report Card . . . 82

6.3.15 Run NYCRR Report Card . . . 83
6.3.16 Run PCI DSS Report Card . . . 84
6.3.17 Run Singapore Standard Report Card . . . 85
6.3.18 Run SOX Report Card . . . 86
7. Report History . . . 88
7.1 Working with Report and Report Card History . . . 89
7.2 Display Report History . . . 90
7.3 Display Report Details . . . 92
7.4 Re-display a Report Output . . . 93
7.5 Re-run Report . . . 94
8. Report Outputs . . . 95
8.1 Working with Report Outputs . . . 96
8.2 Display Report Failure Details . . . 98
8.3 Resolve Report Failures . . . 99
9. Job Activity Monitor . . . 100
9.1 Working with Job Activity Monitor . . . 101
9.2 Display Job Activities . . . 102
9.3 Manage Subsystems . . . 105
9.4 Manage Commands . . . 107
9.5 Manage Activity Monitor Rules . . . 109
9.6 Manage User Groups . . . 111
9.7 Archive Job Activity Data . . . 113
9.8 Run Job Activity Reports . . . 114
10. Authority Collection . . . 116
10.1 Working with Authority Collections . . . 117
10.2 Display Authority Collections . . . 118
10.3 Manage Authority Collection . . . 120
10.4 Run Authority Collection Reports . . . 122
11. Alerts . . . 126
11.1 Working with Alerts . . . 127
11.2 Manage Alerts . . . 128
12. Troubleshooting . . . 129
12.1 TGAudit FAQs . . . 130
12.2 Error Messages . . . 131
13. APPENDICES . . . 132
13.1 APPENDIX - Collectors . . . 133
13.2 APPENDIX - Revision History . . . 142
13.2.1 Version 2.2 - TGAudit User Guide . . . 143
13.2.2 Version 2.1 - TGAudit User Guide . . . 145
13.3 APPENDIX - TG Fix . . . 147
13.4 APPENDIX - TG Job Scheduler . . . 148
13.5 APPENDIX - TG Journal Cleanup . . . 149
13.6 APPENDIX - TG Management . . . 150
13.7 APPENDIX - TG Report Cleanup . . . 151
13.8 APPENDIX - TG Save and Restore . . . 152

What's New

Version 2.2

This release includes the following:

Alert Defaults

You can now set up alerts defaults.

Job Scheduler

You can now set up a job scheduler.

Collectors

The following new collectors are now available:

- AUTHORITY_COL_ALI
- AUTHORITY_COL_IFS
- AUTHORITY_COL_OBJECT
- DATABASE_ACCESS
- DATABASE_OPERATIONS
- DTBASE_OPERATIONS_JRN
- QHST_MSG_INFO
- SENSITIVE_DATABASE_CONTENT

Authority Collection Reports

The following Authority Collection reports are now available:

- Authority Collection for Object IFS Report
- Authority Collection for Object Native Report
- Authority Collection Report (*ALL)

Configuration Reports

The following new Configuration reports are now available for use:

- QHST Message Information
- QHST Messages with Severity Greater Than 40

Data Level Reports

The following Data Level reports are now available.

- Database Access
- Database Operations
- Database Operations by Journal

Resource Reports

The following Resource reports are now available:

- Changed Data Files in Last 30 Days
- Damages Objects
- Files Not Used in the Last 30 Days
- Journaled Files
- New Data Files in Last 30 Days
- New Library in Last 30 Days
- New Objects in the Last 30 Days
- Object Source
- Objects Changed in the Last 30 Days
- Objects Created in the Last 30 Days
- Objects Larger than 100MB
- Objects Owned by QSECOFR
- Objects Used in the Last 30 Days
- Restored Objects in the Last 30 Days
- Source Changes in Last 30 Days
- Unsaved Objects in the Last 30 Days

TGAudit Introduction

TGAudit introduces the next generation of system security audit reporting, data-level reporting, and job activity monitoring to IBM i and iSeries systems. Helping overcome the challenges of internal and external audit requirements, as well as regulatory compliance mandates, TGAudit simplifies data collection with its robust reporting engine, built-in knowledge, and flexible output options.

With over 230 reports delivering built-in security content and predefined Report Card mappings to major compliance regulations such as PCI, HIPAA, and SOX, TGAudit supplies a wealth of knowledge to help you easily gain a comprehensive view of your overall system security and assess the risk of potential security vulnerabilities. Recognizing the many unique facets of each organization, TGAudit also comes equipped with over 100 data source collectors which can be used to customize unique reports as needed. Content can be copied to leverage built-in security knowledge, then adjusted to suit custom needs, or brand-new content can be created from scratch.

Report Cards are an easy way to view high-level pass/fail results of multiple reports at once and maintain an overall security perspective of a server, enabling quick identification of problematic areas as they may arise. With easy to read HTML output, avoid the hassle of digging through numerous spooled files or output files and simply click on hyperlinks to see detailed information for reports with a fail status.

Data-level reporting provides detailed viewing of file changes down to the field level, with the ease of simply running reports over any files that have journaling already started. Cryptic journal data is quickly converted into readable reports showing before and after images of file record details.

For those special cases where additional job-level detailed monitoring is required, the Job Activity Monitor provides a granular approach at capturing interactive and batch job information to help meet auditing requirements, especially of high-privileged users and sensitive jobs. Configure rules to customize the level of logging required for particular users and produce detailed or summary reports in various output types for distribution or view job activity in an interactive work screen.

With the combination of flexibility, knowledge, and powerful efficiency built into TGAudit, it provides the reporting utilities required to maintain an optimal level of security on any IBM i or iSeries server.

> **Note**: While you can use TGAudit as a standalone product, it is also one component of a powerful security suite. For more information about the suite or other products in the suite, go to TrinityGuard.com.

See also

What's New

Setup

Getting Started

Benefits

- Easily assess security vulnerability risks
- Quickly prepare for audits
- Minimize security breaches
- Save hundreds of hours creating reports and researching security requirements
- Easily maintain visibility of system security
- Gain confidence in the level of security enforced on a system
- Save time identifying problematic areas with high-level views
- Ease of ensuring system resource security is maintained
- Quickly identify field-level changes to sensitive files without having to decipher journal data
- Built-in knowledge to assist in achieving regulatory compliance for any of the following regulations:
  - PCI DSS (Payment Card Industry Data Security Standards)
  - HIPAA (Health Insurance Portability and Accountability Act)
  - SOX (Sarbanes-Oxley Act)
  - GLBA (Gramm-Leach-Bliley Act)
  - FISMA (Federal Information Security Management Act)
  - Standards Australia
  - ISO 27001

See also

TGAudit Introduction

Features

- Over 230 reports providing built-in security auditing content
- Predefined report cards that map IBM i security auditing data to several major regulatory compliance regulations
- Robust reporting engine with a wide range of data sources
- Highly customizable report features, including column selection
- Sophisticated report filtering mechanism with SQL-like operators and up to 5 levels of nesting
- Efficient reporting with run-time optimization options
- Enhanced output options (i.e., HTML, CSV, and XML)
- Data sorting in HTML output
- Interface and reporting for IBM i 7.3 Authority Collection security feature
- OS currency

See also

TGAudit Introduction

Setup

This section contains the following topics:

- Configure TGAudit
- Log Into TGAudit
- Set Up Alert Defaults
- Set Up Data Area Journaling
- Set Up Database Journaling
- Set Up Integrated File System Auditing
- Set Up Job Scheduler
- Set Up Object Auditing
- Set Up Range of Journal Receivers for Reports
- Set Up System Auditing
- Clean Up Journal Receivers
- Clean Up Report Data

Configure TGAudit

This section describes the tasks you need to perform to configure TGAudit prior to use.

> **Tip**: You should complete these tasks before running any reports. If auditing is not enabled and configured properly, which includes identifying the auditing journal, no transactions will be captured for reporting purposes. Therefore, reports will be blank (include no data).

To set up TGAudit, access the **Audit Configuration** interface.

To access the Audit Configuration interface

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

2) At the **Selection or command** prompt, enter **1** (TGAudit).

3) Press **Enter**. The **TGAudit - Main** menu is displayed.

4) Press **Enter**.

5) At the **Selection or command** prompt, enter **32** (Audit Configuration). The **Audit Configuration** interface is displayed.

See also

Setup

Log Into TGAudit

Use this task to log into TGAudit from the **IBM i Main** menu.

To access the TGAudit Main menu

1) Sign into your IBM i server.
2) At the **Selection or command** prompt, enter **TGMENU**.
3) Press **Enter**. The **TG Main** menu is displayed.
4) At the **Selection or command** prompt, enter **1** (TGAudit). The **TGAudit Main** menu is displayed.

See also

Setup

Set Up Alert Defaults

Use this task to set up how alerts are handled when triggered by a report.

> **Note**: See Manage Custom Reports for instructions on how to enable alerts.

To set up alert defaults

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **10** (Alert Defaults). The **TGAudit Alert Defaults** interface is displayed.

5) Complete the following fields:

Field	Description
Alert Status	Enter ***YES** to enable alerts (global setting). **Note**: This is a global toggle setting that disables/enables report alerting. If set to ***NO**, then no alerts are triggered regardless of report-specific (local) settings. If set to ***YES**, then when alerting is enabled for a specific report (local setting), then the following information is used for storing any triggered alerts.
Alert Message Queue	Enter the queue in which to store triggered alerts
Alert Message Queue Library	Enter the library in which the message queue resides

See also

Setup

Set Up Data Area Journaling

Use this task to start auditing a data area, which is a form of object. After journaling begins for a data area, you can produce reports that identify changes occurring to that data area.

To set up data area journaling

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **6** (Set up Data Area Journaling). The **Start Journal Object** interf ace is displayed.

Alternatively, use the **STRJRNOBJ** command to access this interface.

5) Modify the data area journaling attributes as necessary.

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

Note: The system captures before and after images of changes to the data area. To view these changes, run the **Da ta Area Changes** reports available in the **Data Level Reports** menu.

See also

Setup

Set Up Database Journaling

Use this task to start auditing DB2 database files on the system. After journaling begins for a physical file, you can produce reports that identify changes occurring to the database.

To set up database journaling

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **5** (Set up Database Journaling). The **Start Journal Physical File** interface is displayed.

Alternatively, use the **STRJRNPF** command to access this interface.

5) Modify the database journaling attributes as necessary.

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

> **Note**: The system captures before and after images of changes to the database. To view these changes, run the **Database Changes** reports available in the **Data Level Reports** menu.

See also

Setup

Set Up Integrated File System Auditing

Use this task to set up configure auditing for the Integrated File System (IFS), which is a form of object.

To set up IFS auditing

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **4** (Set up Integrated File System Auditing). The **Change Auditing Value** interface is displayed.

Alternatively, use the **CHGAUD** command to access this interface.

5) Modify the IFS attributes as necessary.

Field	Description
Object	Path to the IFS directory you want to monitor (e.g., /home/*)
Object auditing value	The activity you want to monitor (e.g., who has viewed the object, who has changed the object, etc.)
Directory subtree	Directory subtrees you want to monitor
Symbolic link	Whether to monitor just the specific IFS object (*NO) or whether to monitor all objects (*YES) associated with a symbolic link

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

See also

Setup

Set Up Job Scheduler

Use this task to select the desired job scheduler.

To select a job scheduler

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **11** (Job Scheduler Details).

5) Complete the following fields:

Field	Description
Current Job Scheduler?	Identify the desired job scheduler: ***IBM** - IBM Scheduler ***IBMAJS** - IBM Advanced Job Scheduler ***ROBOT** - Robot Scheduler

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

See also

Setup

Set Up Object Auditing

Use this task to set up object level auditing for specific sensitive objects that require close monitoring.

To set up object auditing

1) Access the **TG Audit Main** menu.

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **3** (Set up Object Auditing). The **Change Object Auditing** interface is displayed.

Alternatively, use the **CHGOBJAUD** command to access this interface.

5) Modify the object attributes as necessary.

Field	Description
Object	Name of the object you want to monitor (audit)
Library	Library in which the object resides
Object type	Type of object
ASP Device	Name of auxiliary storage pool
Object auditing value	Activity you want to monitor

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

Important: To enable object-level auditing, the system value **QAUDCTL** must also be set to include the value ***OBJAUD**.

Tip: You can set the **QAUDCTL** system value using option **2** (Change Security Auditing).

See also

Setup

Set Up Range of Journal Receivers for Reports

Use this task to configure the journal receiver range (threshold). The range determines how much transactional data from a journal should be stored in each receiver.

> **Note**: If and when the threshold is reached, the system automatically generates a new receiver. Each new receiver is numbered sequentially.

To set up range for journal receivers

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **7** (Set up Range of Journal Receivers for Reports). The **Start Journal Object** interface is displayed.

Alternatively, use the **TGJRNATR** command to access this interface.

5) Modify the range attributes as necessary.

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

See also

Setup

Set Up System Auditing

Use this task to ensure that system auditing is enabled before running auditing reports. Reports will not contain pertinent data until system auditing is enabled and configured.

The following tasks are described:

- Display Security Auditing Journal Details
- Change Security Auditing

To modify system security, access the **Audit Configuration** (TGMAUDCFG) interface. This screen provides access to system commands that allow you to modify security audit settings. Once configured, you will have access to pertinent security audit data.

> **WARNING**: Audit configuration changes affect the whole system and are not local to just TG products. Therefore, communicate with your operations team and arrange for storage of the security audit journal receivers. The size requirements for the journal receivers is based on the unique needs of your environment, the auditing required that meet your security policy, and the amount of usage on the server.

Display Security Auditing Journal Details

Use this task to display the details associated with the security auditing journal (QAUDJRN).

To display the security audit journal details

1) Sign into your IBM i server.

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

3) At the **Selection or command** prompt, enter **1** (TGAudit) to access the **Main** menu.

4) At the **Selection or command** prompt, enter **32** (Audit Configuration).

5) Press **Enter**.

6) At the **Selection or command** prompt, enter **1** (Security Auditing Journal Details).

Change Security Auditing

Use this task to change security auditing definitions to meet your security policy requirements.

To change security auditing

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **2** (Change Security Auditing). The **Change Security Auditing** interface is displayed

Alternatively, use the **CHGSECAUD** command to access this interface.

Note: If the security audit journal (QAUDJRN) does not exist when the **CHGSECAUD** command is issued, the system creates the journal along with its initial journal receiver. Audit data gathered due to the configuration of this command is stored in the QAUDJRN journal receiver.

5) Enter the options that best meet your security policy requirements.

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

Tip: If you receive the message **Object QAUDJRN in library *LIBL not found**, it means auditing is not set up, so there is no visibility into security-related activity happening on the system.

Important: If the QAUDJRN is absent or not properly set up, many reports will not return data.

See also

Setup

Clean Up Journal Receivers

Use this task to cleanup journal receivers. Journal receivers tend to consume a lot of disk space and, depending on your system activity, can grow very fast.

> ⚠ **Important**: Before using this tool, review your data retention policy and make a backup of the receivers for later retrieval. In case of a security incident investigation, old receiver data is required for forensic analysis.

To perform journal receiver cleanup

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **8** (Journal Receiver Cleanup).

5) Complete the following fields:

Field	Description
Journal	Enter the journal name from which journal receivers are to be deleted.
Library	Enter the name of the library where the journal resides. The possible values are: ***LIBL** All libraries in the library list are searched to locate the journal. ***CURLIB** The current library is used to locate the journal. **name** Specify the library where the journal is located.
Journal data retention days?	Enter the number of days of journal data you want to retain. For example, if you specify 60 days, you will retain all journal receivers containing the last 60 days of journal data. Valid values are 1 - 99999.
Delete unsaved data?	Enter whether or not only journal data previously saved to media will be deleted. The possible values are: ***NO** Only data previously saved to media will be deleted. ***YES** Journal data associated with the journal will be deleted regardless of if it was previously saved.
Run interactively?	Enter whether you want the journal cleanup job to run in batch or interactively. Consider the amount of journal data needing to be deleted when deciding whether to run interactively or in batch. Very large amounts of data to delete could take a long time to run. The possible values are: ***NO** Submits the TGJRNCLEAN command to run in batch mode. ***YES** Executes the TGJRNCLEAN command interactively.
Job Queue	Enter the job queue in which the job will be queued to run. This parameter is only valid for batch jobs. The possible values are: **QBATCH** The name of the job queue where the job processing this command will be placed. "QBATCH" is the default name of the job queue, but this name can be changed. ***NONE** The job data will not be placed in a job queue.

Library	Enter the library where the job queue resides. This parameter is only valid for batch jobs. The possible values are: ***LIBL** All libraries in the library list are searched to locate the job queue. ***CURLIB** The current library is used to locate the job queue. **name** Specify the library where the job queue is located.
Schedule job?	Enter whether you want to use IBM's job scheduler to schedule journal cleanup or to have the job run in batch mode. The possible values are: ***NO** The job is not scheduled. ***YES** The job is scheduled using IBM's job scheduler. The default job name given is TGJRNCLEAN. IBM job scheduler options are displayed and can be edited as desired.

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

6) Click **Enter**.

See also

Setup

APPENDIX - TG Journal Cleanup

Clean Up Report Data

Use this task to manage HTML report data stored in the IFS. You can purge report data automatically on a scheduled basis using this tool.

To perform report data cleanup

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

2) At the **Selection or command** prompt, enter **32** (Audit Configuration).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **9** (Report Data Cleanup).

5) Complete the following fields.

Field	Description
Report data retention days?	Enter the number of days you want to retain the report data. For example, if you specify 60 days, you will retain report data for the last 60 days. Valid values are 1 - 99999
Archive?	Enter whether you want to archive incoming transaction data. ***NO** - do not archive ***YES** - archive

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

See also

Setup

APPENDIX - TG Report Cleanup

Getting Started

This section includes the following topics:

- Use TGAudit

Use TGAudit

Beginning by running built-in reports and built-in report cards designed by security experts to identify security issues:

- Working with Reports
- Working with Report Cards
- Working with Report History
- Working with Report Outputs

Then create custom reports specific to your organization to expand your security visibility:

- Working with Custom Reports
- Working with Custom Report Cards

Finally, use what you have learned to improve your security strategy:

- Working with Job Activity Monitor
- Working with Authority Collections
- Working with Product (TG) Management

See also

Setup

Reports

This section describes how to work with **Reports**.

This section includes the following topics:

- Built-in Reports
- Custom Reports
- Authority Collection Reports
- Data Level Reports
- Security and Configuration Reports

See also

TGAudit Report Reference Guide

Built-in Reports

This section describes how to work with **Built-in** reports.

- Working with Reports
- Display List of Reports
- Run Reports

See also

Reports

TGAudit Report Reference Guide

Working with Reports

This section describes working with built-in reports.

- Display List of Reports
- Run Reports

> **Note**: To work with built-in reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

> **Tip**: See the **TGAudit Report Reference Guide** for details about a specific report.

See also

Built-in Reports

TGAudit Report Reference Guide

Display List of Reports

Use this task to do the following:

- Display list
- Sort List
- Move to Location in List
- Filter List

Display list

Use this task to display the list of available reports.

To display the list of reports

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

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

Sort List

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

To sort the list

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

2) Place your cursor on a column heading (e.g., Collector ID, Report Name, or Category).

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

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

Move to Location 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 locate a report.

To move to a specific position within the list

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

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

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

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

Filter List

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

To filter the list using a subset

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

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

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

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

See also

Working with Reports

Working with Report Outputs

TGAudit Report Reference Guide

Run Reports

Use this task to run a built-in or custom report using the **Work with Reports** interface:

> **Note**: See the **TG Audit Report Reference Guide** for information about individual reports.

- Run Reports with Start and End Time Requirements
- Run Reports without Start and End Time Requirements

> **Tip**: You can schedule reports to run when most convenient.

Run Reports with Start and End Time Requirements

Use these instructions when the report requires a start and end time entries.

Identifying a start and end time helps you filter the data reported and is required for some types of reports that have the potential to contain a huge amount of data.

To run a report with start and end time requirements

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

4) Enter **7** in the **Opt** column for the report you want to run.

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

Field	Description
Collector ID	ID identifying the collector from which report data is obtained (not an editable field)
Collector Name	Name assigned to the collector (not an editable field)
Report ID	ID assigned to the report you want to run (not an editable field)
Starting date	Select from the options available: ***CUR** - Use the current date ***CMS** - Use the current month's start date ***LMS** - Use the last month's start date ***LME** - Use the last month-end date ***LYS** - Use the last year's start date ***LYE** - Use the last year's end date ***LWS** - Use the last week's start date (last 7 days) ***LDS** - Use the last day's start date

Starting time	Enter time in the format (hhmmss): hour, minute, second
Ending date	Select from the options available
Ending time	Enter time in the format (hhmmss): hour, minute, second
Override report defaults?	Whether to override report defaults: ***YES** - Ignore run-time collector defaults ***NO** - Apply Run-time collector defaults
Reload collector data	Whether to reload the collector data: ***AI** - Allow the artificial intelligence engine to determine if data source collection should be re-run ***YES** - Re-run data source collection before producing the report output ***NO** - Used cached version of the data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
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.

Run Reports without Start and End Time Requirements

Use these instructions when the report does not require a start and end time.

To run a report without start and end time requirements

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

4) Enter **7** in the **Opt** column for the report you want to run.

5) Press **Enter**.

6) Modify the run criteria as necessary.

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

Field	Description
Collector ID	ID identifying the collector (not an editable field)
Collector	Name assigned to the collector (not an editable field)
Report ID	ID assigned to the report you want to run (must be a report associated with the collector) **Note**: Multiple reports can be produced from a single collector, so at this point, you could change the report ID to any of the reports linked to the identified collector.

Override report defaults	Whether to override report defaults: ***YES** - Ignore run-time collector defaults ***NO** - Apply Run-time collector defaults **Tip**: Run-time collector defaults maximize report efficiency. Collector defaults allow you to filter collector data before attempting to generate your report. **Note**: See Create Report for additional information about setting up run-time collector defaults.
Reload collector data	Whether to reload the collector data: ***AI** - Allow the artificial intelligence engine to determine if data source collection should be re-run ***YES** - Re-run data source collection before producing the report output ***NO** - Used cached version of the data source collection
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
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.

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

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

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

See also

Working with Reports

Working with Report Outputs

TGAudit Report Reference Guide

Custom Reports

This section describes how to work with **Custom** reports.

- Working with Custom Reports
- Create Custom Reports
- Manage Custom Reports
- Run Custom Reports

See also

Reports

Working with Custom Reports

This section describes working with custom reports:

- Create Custom Reports
- Manage Custom Reports
- Run Custom Reports

> **Note**: To work with custom reports, access the **Work with Reports** interface.

To access the Work with Reports interface

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

2) At the **Selection or command** prompt, enter the **30** (Work with Reports).

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

See also

Custom Reports

Create Custom Reports

Use this task to create a custom report. Creating a report is a multi-step process:

- Access the Work with Reports Interface
- Add Report
- Select Data Source Collector
- Name the Report
- Select Report Fields
- Change Order of Fields
- Define Report Filter Criteria
- Define Run-time Collector Defaults
- Confirm Report Creation

Access the Work with Reports Interface

To create reports, access the **Work with Reports** interface.

To access the Work with Reports interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**.

Add Report

Use this task to add a report.

To add a Report

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

2) Press the **F6** (Add Report) function key on your keyboard.

3) Follow the steps in the report wizard.

Select Data Source Collector

Use this task to select the data source collector for your custom report. Each report must have a least one source (collector) from which to pull data.

To select the data source collector

1) In the **Opt** column for the collector that you want to use as the data source for your report, enter **1** (Select).

2) Press **Enter**.

Name the Report

Use this task to assign a name, ID, and category to your custom report.

To identify the report

1) Complete the following fields:

Field	Description
Report ID	ID you want to assign to the report **Tip**: The name cannot contain spaces.
Report Name	Name that you want to assign the report **Tip**: Use a name that describes the data that will appear in the report.
Category	The report category under which you want to group the report **Tip**: There are four standard categories: Configuration, Resources, Profiles, Network.

2) Press **Enter**.

> **Note**: The report should now be linked to the collector and appear in your list of available reports under the identified category.

Select Report Fields

Use this task to select the collector fields that you want to appear as columns in your report.

> **Note**: By default, all collector fields are selected when you create a custom report.

> **Tip**: To customize which collector fields to include, press the **F4** (Select Fields) function key on your keyboard.

To select report fields

1) Press the **F4** (Select Fields) function key on your keyboard.

2) Enter **1** in the **Sel** column for each field you want to include as a column in your custom report.

3) Press **Enter**.

Change Order of Fields

To change the order of the selected fields

Use this task to define the order in which fields should appear in the report.

> **Tip**: The column with the lowest sequence number appears as the first column. The column with the highest sequence number appears as the last column.

1) Adjust the sequence numbers in the **Seq** column.

2) Press **Enter**.

Define Report Filter Criteria

Use this task to define the filter criteria for your custom report.

> **Note**: Filters are not necessary but might improve the performance of your report.

To build report filter criteria

1) Press the **F4** (Select Fields) function key on your keyboard.

2) Enter **1** in the **Sel** column for each field to which you want to apply a filter.

3) Press **Enter**.

To add filter criteria

1) Add operators and comparison values as necessary.

2) Press **Enter**.

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

> **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.

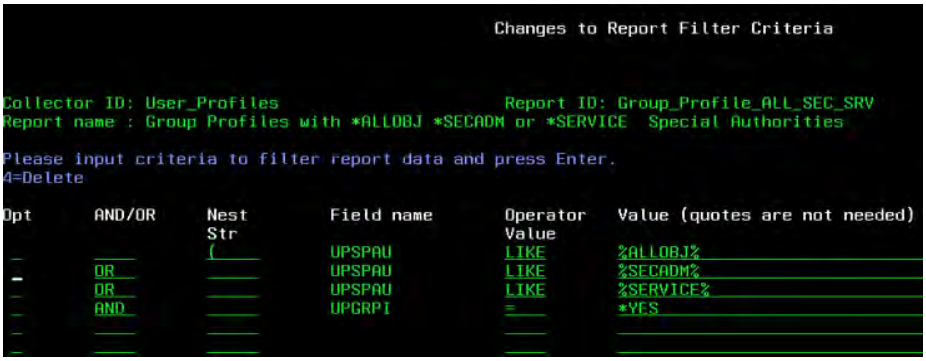


Figure: Build Report Filter Criteria

To delete filter criteria

1) Enter **4** (Delete) in the **Opt** column for the filter criteria you want to delete.

2) Press **Enter**.

Define Run-time Collector Defaults

Use this task to customize the defaults for the data source collection. This enables you to maximize how efficiently the report runs. Report defaults provide options specific to the data source collector on which the report is based, so you can filter the actual data source before the report filter is even applied.

An example of when report defaults are very useful is in the case of reports based on QAUDJRN journal data or database file journal data, where very large amounts of data can potentially accumulate and take a long time to process in a typical reporting scheme. With report defaults, you can specify particular date ranges so that any report filters are only run across a subset of data instead of the entire range of available data.

Report defaults are processed before any report run-time options, except when a user selects ***YES** in the **Override report defaults** field at the time they run a report.

> **Note**: See Run Reports for additional information about the **Override report defaults** field.)

> **Tip**: Collector defaults are highly recommended, but they are not required. Click the **F2** function key to skip this step.

To define report defaults

1) Enter the desired run-time collector default values.

2) Press **Enter**.

Confirm Report Creation

Use this task to confirm that you want to create the report that you have just defined.

> **Tip**: Click the **F12** function key to go back one step at a time if you want to make changes or verify that you entered the correct information.

To confirm report creation

1) Review the information.

2) Press **Enter**.

See also

Working with Custom Reports

Manage Custom Reports

Use this task to do the following:

- Access the Work with Reports Interface
- Edit Report
- Copy Report
- Delete Report
- Enabling Report Alerting

To manage reports, access the **Work with Reports** interface.

Access the Work with Reports Interface

To access the Work with Reports interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

3) Press **Enter**. The **Work with Reports Interface** is displayed.

Alternatively, at the IBM i command line, enter **TGWRKRPT**, and press **Enter**.

Edit Report

Use this task to edit a custom report.

Tip: You cannot edit built-in reports, but you can create a copy of a built-in report and then edit the copy.

Important: The **Report ID** cannot be edited after the report is created.

To edit a report

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

2) Enter the appropriate option in the **Opt** column for the report you want to modify:

Option	Description
2 (Edit)	Modify the report name, category, and regulation details **Note**: Only available for Custom Reports, not built-in reports (those shipped with the product)
5 (Alerts)	Modify the condition (number of rows returned) that trigger the generation of an alert
6 (Defaults)	Modify the run-time collector defaults, which help to filter collector data **Note**: See Create Reports for additional information about run-time collector defaults.

8 (Field List)	Modify which collector fields you want to display in your report **Note**: Modifications cannot be made to built-in reports
9 (Filter)	Modify the filters you want applied to the data obtained from the collector **Note**: Modifications cannot be made to built-in reports

Copy Report

Use this task to copy a report. This is useful when an existing report provides results that are close to what you need, but still do not quite meet your requirements. You can save time by copying the report and customizing it instead of beginning from scratch.

To copy a report

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

2) In the **Opt** column for the report you want to copy, enter **3** (Copy).

3) Enter a unique Report ID and continue customization as desired. Please refer to "Creating Reports" for details.

Delete Report

Use this task to delete a report.

> **Note**: You can delete only customer reports, not built-in reports.

To delete a report

1) Acesss the **Work with Reports** interface.

2) In the **Opt** column for the report you want to delete, enter **4** (Delete).

Enabling Report Alerting

Use this task to enable alerting based on the results (number of rows) produced in a given report. This is useful if you want the system to send a notification when the number of rows in a report exceeds a threshold.

> **Tip**: You can set up alerts for both built-in and custom reports.

To enable report alerting

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

2) In the **Opt** column for the desired report, enter **5** (Alerts).

3) Complete the following fields:

Field	Description
Alert Status	Enter ***YES** to enable alerts for this specific report (local setting)

Alert Criteria (Condition)	Enter the desired mathematical symbol (<, >, =, etc.)
Alert Criteria (No. of Rows)	Enter the number of rows used in conjunction with a mathematical symbol to determine the threshold used to trigger an alert (e.g., if the number of rows is > 10, then trigger an alert). **Note**: See Set Up Alert Defaults for instructions on defining the action taken when a report triggers an alert.

See also

Working with Custom Reports

Run Custom Reports

Use this task to run a custom report card.

To run a custom report

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **30** (Work with Reports).

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

4) In the **Opt** column for the report you want to copy, enter **7** (Run).

5) Modify the run criteria and output option as necessary

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

6) Press **Enter**.

See also

Working with Custom Reports
Working with Regulation Report Cards

Authority Collection Reports

This section describes how to manage **Authority Collection** reports.

- Working with Authority Collection Reports

See also

Reports

TGAudit Report Reference Guide

Working with Authority Collection Reports

Authority Collection reports contain information about authorities assigned to objects and users.

This section describes working with the following reports:

- Authority Collection for Object IFS Report
- Authority Collection for Object Native Report
- Authority Collection for Users and IFS Report
- Authority Collection for Users and Native Object Report
- Authority Collection Report (*ALL)

Tip: See the TGAudit Report Reference Guide for a description of individual reports.

Note: To work with authority collection reports, access the **Authority Collection Reports** interface.

To access the Authority Collection Reports interface

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

2) At the **Selection or command** prompt, enter the **4** (Authority Collection).

3) Press **Enter**. The **Authority Collection** interface is displayed.

4) At the **Selection or command** prompt, enter the **20** (Authority Collection Reports).

5) Press **Enter**. The **Authority Collection Reports** interface is displayed.

See also

Authority Collection Reports

Data Level Reports

This section describes how to manage **Data Level** reports.

- Working with Data Level Reports

See also

Reports

TGAudit Report Reference Guide

Working with Data Level Reports

Data Level reports contain information about data areas and files.

> **Tip**: These reports require system auditing to be enabled.

This section describes working with the following reports:

- Cross Reference Physical Files
- Data Area Changes
- Database Access
- Database Changes
- Database Content
- Database Operations
- Database Operations by Journal
- Field Level Authorities
- Row and Column Access Control
- Schedule Master File
- Sensitive Database Content

> **Tip**: See the TGAudit Report Reference Guide for a description of individual reports.

> **Note**: To work with security and configuration reports, access the **Data Level Reports** interface.

To access the Data Level Reports interface

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

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

3) Press **Enter**. The **Data Level Reports** interface is displayed.

See also

Data Level Reports

Security and Configuration Reports

This section describes how to work with **Security** and **Configuration** reports.

- Working with Security and Configuration Reports

See also

Reports

TGAudit Report Reference Guide

Working with Security and Configuration Reports

The **Security** and **Configuration** reports are for reporting various configuration settings associated with the system, or authorities, or various profile parameters, etc.

This section describes working with the following reports:

- Configuration Reports
- Profile Reports
- Network Reports
- Resource Reports

Tip: See the TGAudit Report Reference Guide for a description of individual reports.

Note: To work with security and configuration reports, access the **Security and Configuration Reports** interface.

To access the Security and Configuration Reports interface

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

2) At the **Selection or command** prompt, enter the **1** (Security and Configuration Reports).

3) Press **Enter**. The **Security and Configuration Reports** interface is displayed.

See also

Security and Configuration Reports

Report Cards

This section describes how to work with **Report Cards**.

- Built-in Report Cards
- Custom Report Cards
- Regulation Report Cards

Built-in Report Cards

This section describes how to work with **Built-in** report cards:

- Working with Report Cards
- Display list of report cards
- Run report cards

See also

Report Cards

Working with Report Cards

This section describes working with customer report cards:

- Display list of report cards
- Run report cards

> **Note**: To work with built-in report cards, access the **Work with Report Cards** interface.

To access the Work with Report Cards interface

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

2) At the **Selection or command** prompt, enter the **31** (Work with Report Cards).

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

See also

Built-in Report Cards

Display List of Report Cards

Use this task to do the following:

- Display list
- Sort List
- Move to Location in List
- Filter List

Display list

Use this task to display the list of available reports.

To display the list of report cards

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **3** (Work with Report Cards).

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

Sort List

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

To sort the list

1) Access the **Work with Report Cards** interface.

2) Place your cursor on a column heading.

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

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

Move to Location 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 locate a report.

To move to a specific position within the list

1) Access the **Work with Report Cards** interface.

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

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

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

Filter List

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

To filter the list using a subset

1) Access the **Work with Report Cards** interface.

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

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

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

See also

Working with Reports

Working with Report Outputs

Run Report Cards

Use this task to run a report card using the **Work with Report Cards** interface, which allows you to configure (i.e., edit, copy, etc.) report card.

To run a report using the Work with Report Cards interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).

3) Press **Enter**.

4) In the **Opt** column for the report you want to run, enter **7** (Run).

5) Press **Enter**.

6) Modify the run criteria and output option as necessary.

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

See also

Working with Report Outputs

Custom Report Cards

This section describes working with **Custom** report cards. A report card is a compilation of reports, grouped to run all at the same time, to produce a high-level view of the **Pass/Fail** status achieved from each report run from within the report card. Depending on the reports included, you might also see **INFO** in the status column instead of **PASS** or **FAIL**. This indicates that the value in the **Number of Violations** column is for information purposes only and does not trigger the passing or failing of the report.

> **Tip:** Report cards are intended to be run using the *HTML output view. This allows you to see the output in a web browser and drill down to see the details of any reports that return a fail status.

There are several built-in report cards shipped with the product that map to many widely used compliance regulations. You can also create your own report cards and customize the reports, pass/fail criteria, and regulation clauses contained in it. To help aid the process of customization, you can also copy a built-in report card and edit it as desired, since built-in report cards cannot be edited.

This section includes the following topics:

- Working with Custom Report Cards
- Create Custom Report Cards
- Manage Custom Report Cards
- Run Custom Report Card

See also

Report Cards

Working with Custom Report Cards

This section describes working with customer report cards:

- Create Custom Report Cards
- Manage Custom Report Cards
- Run Custom Report Card

> **Note**: To work with custom report cards, access the **Work with Report Cards** interface.

To access the Work with Report Cards interface

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

2) At the **Selection or command** prompt, enter the **31** (Work with Report Cards).

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

See also

Custom Report Cards

Create Custom Report Card

Use this task to create a customer report card. This task involves multiple steps.

- Define Report Card Name
- Define Report List
- Define Pass Criteria
- Define Regulation Clause

Define Report Card Name

Use this task to assign the report card a name.

To define the report card name

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).

3) Press **Enter**.

4) Press the **F6** (Add Report Card) function key on your keyboard.

5) Enter the following:

   – **Report Card ID** – which should not contain spaces

   – **Report Name** – which should describe reports included in the report card

   – **Category** – which should identify the category (e.g., Regulations) under which the report card will reside.

6) Enter a **Y** in the **Regulation** parameter if the report contains regulatory reports. This can help you map reports to particular sections of a compliance regulation document or security policy. Otherwise, enter **N**.

7) Press **Enter** twice.

Define Report List

Use this task to add reports to the report card.

To add reports to the report card

1) Access the **Work with Report Cards** interface.

2) In the **Opt** column for the report card you want to modify, enter **9** (Select Reports).

3) Press the **F4** (Select Report) function key on your keyboard. The **Select** screen is displayed.

4) Select the reports you want to include in the report card by entering an **X** in the **Sel** column.

5) Press **Enter**.

Define Pass Criteria

Use this task to define the pass criteria. After all reports are selected, define the pass criteria. A comparison condition and the number of rows returned in the report make up the pass criteria.

For example, the **User Profile Changes** report returns rows any time a user profile on the system is changed. It is good practice to be aware of and review any user profile changes to ensure they adhere to your security policy. Therefore, you could set the pass criteria for the report as the number of rows must be less than 1 to return the report status of **Passed**. Then when you run the report card, if the number of rows in the **User Profile Changes** report is greater than one, the report card will return a status of **Failed**.

> **Tip**: An SQL-like format is used to create pass criteria. For a list of supported operators, press **F10**.

To define the pass criteria

1) Enter the operator in the **Comp Cond** column.

2) Enter the criteria in the **Number or Rows** column.

3) Press **Enter**.

Define Regulation Clause

Use this task to identify the regulation clause to which the report card is associated. If you are creating a report card that contains reports that map to a particular compliance regulation or security policy document, use this task to identify the specific clause that each report addresses.

To define regulation clauses

1) Enter the appropriate clause in the **Regulation Clause** column.

2) Press **Enter**.

See also

Work with Custom Report Cards

Manage Custom Report Cards

Use this task to do the following:

- Edit Report Card
- Delete Report Card

Edit Report Card

Use this task to modify a customer report card.

> **Note**: You cannot modify built-in report cards.

To edit a report card

> **Important**: The **Report Card ID** cannot be edited after the report card is created.

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).

3) Press **Enter**.

Alternatively, at the IBM i command line, enter **TGWRKCARD**, and press **Enter**.

4) In the **Opt** column for the report card you want to modify, enter the appropriate option:

Option	Description
2 (Change)	Modify the report card name, category, and regulation details
9 (Select Reports)	Add or remove reports, change pass criteria, and change regulation clause text

Delete Report Card

Use this task to delete a customer report card.

To delete a report

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).

3) Press **Enter**.

Alternatively, at the IBM i command line, enter **TGWRKCARD**, and press **Enter**.

4) In the **Opt** column for the report card you want to delete, enter **4** (Delete).

See also

Work with Custom Report Cards

Run Custom Report Card

Use this task to run a custom report card.

To run a custom report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).

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

4) In the **Opt** column for the report card you want to copy, enter **7** (Run).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

See also

Work with Custom Report Cards

Regulation Report Cards

This section describes working with **Regulatory** report cards. Regulatory report cards are designed around common compliance regulations that are standard for many companies. These built-in regulation report cards assist you with deciphering complex compliance regulation requirements specifically for the IBM i platform, and they allow you to quickly gather data to start evaluating your system. The built-in report cards as available through **Regulation Report Cards** (TGMREG) interface.

This section includes the following topics:

- Working with Regulation Report Cards
- Run Australia Standard report card
- Run COBIT report card
- Run CSA report card
- Run FFIEC report card
- Run FISMA report card
- Run GAPP report card
- Run GLBA report card
- Run HIPAA report card
- Run IRS 1075 report card
- Run ISO 27001 report card
- Run ITIL KPI report card
- Run NERC report card
- Run Nevada Gaming Standard report card
- Run NYCRR 500 report card
- Run PCI report card
- Run Singapore Standard report card
- Run SOX report card

See also

Report Cards

Working with Regulation Report Cards

This section describes working with the following regulation report cards:

- Run Australia Standard report card
- Run COBIT report card
- Run CSA report card
- Run FFIEC report card
- Run FISMA report card
- Run GAPP report card
- Run GLBA report card
- Run HIPAA report card
- Run IRS 1075 report card
- Run ISO 27001 report card
- Run ITIL KPI report card
- Run NERC report card
- Run Nevada Gaming Standard report card
- Run NYCRR 500 report card
- Run PCI report card
- Run Singapore Standard report card
- Run SOX report card

Note: To work with regulation report cards, access the **Regulation Report Cards** interface.

To access the Regulation Report interface

1) Log into to TGAudit. The Main menu appears.

2) At the **Selection or command** prompt, enter **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

See also

Regulation Report Cards

Run Australia Standard Report Card

Standard Australia is the nation's peak non-government standards organization. It is charged by the Commonwealth Government to meet Australia's need for contemporary, internationally aligned standards and related services.

AS/NZS ISO 27037 is the latest standard related to information technology — security techniques — guidelines for identification, collection, acquisition, and preservation of digital evidence.

To run the Standard Australia report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **6** (Standard Australia).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run COBIT 5 Report Card

The Control Objectives for Information and related Technology (COBIT) 5 regulatory standards were created by the Information Systems Audit and Control Association (ISACA).

> **Note**: Go to ISACA.org for additional information about this regulatory standard.

To run the COBIT 5 report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **8** (COBIT 5 Framework).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run CSA Report Card

The Cloud Security Alliance (CSA) regulatory standards were created by CSA.

> **Note**: Go to CloudSecurityAlliance.org for additional information about this regulatory standard.

To run the Cloud Security Alliance report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **10** (Cloud Security Alliance).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run FFIEC Report Card

The FFIEC (Federal Financial Institution Examination Council) regulatory standards were created by FFIEC.

> **Note**: Go to FFIEC.org for additional information about this regulatory standard.

To run the FFIEC Cybersecurity Assessment Tool report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **17** (FFIEC Cybersecurity Assessment Tool).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run FISMA Report Card

The Federal Information Security Management Act (FISMA) of 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.

FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.

According to FISMA, the term *information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Assessment cases can be categorized as follows:

- Access Control
- Awareness and Training
- Audit and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

The American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP) regulatory standards were created by the AICPA.org.

> **Note**: Go to https://www.aicpa.org for additional information about this regulatory standard.

To run the FISMA report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **5** (Federal Information Security Management Act of 2002: FISMA).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run GAPP Report Card

The Generally Accepted Privacy Principles (GAPP) regulatory standards were created by the American Institute of Certified Public Accountants (AICPA).

> **Note**: Go to AICPA.org for additional information about this regulatory standard.

To run the AICPA GARP report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **14** (AICPA GAPP).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run GLBA Report Card

The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, allowed commercial banks, investment banks, securities firms, and insurance companies to consolidate. GLBA compliance is mandatory whether a financial institution discloses nonpublic information or not. There must be a policy in place to protect the information from foreseeable threats in security and data integrity.

Major components put into place to govern the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information include:

- Financial Privacy Rule
- Safeguards Rule
- Pretexting Protection

Financial Privacy and Safeguards Rule:

- 15 USC § 6801 – Protection of nonpublic personal information
- 15 USC § 6802 – Obligations with respect to disclosures of personal information
- 15 USC § 6803 – Disclosure of institution privacy policy
- 15 USC § 6804 – Rulemaking
- 15 USC § 6805 – Enforcement
- 15 USC § 6806 – Relation to other provisions
- 15 USC § 6807 – Relation to State laws
- 15 USC § 6808 – Study of information sharing among financial affiliates
- 15 USC § 6809 – Definitions Pretexting protection
- 15 USC § 6821 – Privacy protection for customer information of financial institutions
- 15 USC § 6822 – Administrative enforcement
- 15 USC § 6823 – Criminal penalty
- 15 USC § 6824 – Relation to State laws
- 15 USC § 6825 – Agency guidance
- 15 USC § 6826 – Reports
- 15 USC § 6827 – Definitions

To run the GLBA report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **4** (Gramm-Leach-Bliley Act: GLBA).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run HIPAA Report Card

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the United States Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The administrative simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

With the vast amount of process transition to meet HIPAA requirements and the monumental move toward electronic processing of healthcare information, it is essential to pay close attention to how patient information is processed.

The security rule within HIPAA governs Electronic Protected Health Information (EPHI) and has three specific areas required for compliance.

- Administrative Safeguards: policies and procedures designed to clearly show how an organization will comply with the act
- Physical Safeguards: controlling physical access to protect against inappropriate access to protected data
- Technical Safeguards: controlling access to computer systems and enabling covered entities to protect communications containing Protected Health Information (PHI) transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

Examples of enforcing compliance to HIPAA regulations include ensuring access to patient information is on a need-to-know basis; putting safeguards in place to uphold the integrity of electronic data and guarantee unauthorized changes and data loss are prevented; significant configuration reporting requirements; documented risk analysis and risk management programs.

Most recently, through the HITECH Act, there are also notification requirements for data breaches where affected individuals, the government, and the media must be made aware of unauthorized access to protected information.

To run the HIPAA report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **2** (Health Insurance Portability and Accountability Act: HIPAA).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description

Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run IRS Publication 1075

The Internal Revenue Service (IRS) 1075 regulatory standards were created by IRS. These standards ensure the protection of federal tax returns.

> **Note**: Go to IRS.org for additional information about this regulatory standard.

To run the IRS Publication 1075 report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **9** (IRS Publication 1075).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run ISO 27001 Report Card

The ISO/IEC 27001 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology – Security techniques – Code of practice for information security management.

After the 3 introductory sections,

- Framework,
- Acceptable Use of Information Technology Resources, and
- Information Security Definition & Terms),

The standard contains the following twelve main sections:

1. Risk assessment
2. Security policy – management direction
3. Organization of information security – governance of information security
4. Asset management – inventory and classification of information assets
5. Human resources security – security aspects for employees joining, moving and leaving an organization
6. Physical and environmental security – protection of the computer facilities
7. Communications and operations management – management of technical security controls in systems and networks
8. Access control – restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance – building security into applications
10. Information security incident management – anticipating and responding appropriately to information security breaches
11. Business continuity management – protecting, maintaining and recovering business-critical processes and systems
12. Compliance – ensuring conformance with information security policies, standards, laws and regulations

To run the ISO 27001 report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **7** (Information Security Management System Standard: ISO 27001).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run ITIL KPI Report Card

The Information Technology Infrastructure Library (ITIL) Key Performance Indicator (KPI) standards were created by the AXELOS. These standards help to prevent identity theft.

> **Note**: Go to AXELOS.com for additional information about this regulatory standard.

To run the ITIL Key Performance Indicator report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **13** (ITIL Key Performance Indicator).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run NERC Report Card

The North America Electric Reliability Corporation (NERC) standards were created by the NERC. These standard protect bulk power systems against cybersecurity threats.

> **Note**: Go to NERC.com for additional information about this regulatory standard.

To run the NERC report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **12** (NERC Critical Infrastructure Protection V5).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run Nevada Standard Report Card

The Minimum Internal Control Standards (MICS) were created by the Nevada Gaming Commission and the Nevada Gaming Control Board. These standards help to reduce the risk of loss because of customer or employee access to cash or cash equivalents in gambling establishments.

> **Note**: Go to gaming.nv.gov for additional information about this regulatory standard.

To run the Nevada Gaming Standards report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **15** (Nevada Gaming Minimum Internal Control Standards).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run NYCRR Report Card

The New York Code Rules and Regulations (NYCRR) Section 500 standards were created by the New York State Department of State's Division of Administrative Rules. These standards help to reduce cybersecurity loss in the Financial Services Industry (FSI) in New York.

> **Note**: See DFS.NY.gov for additional information about this regulatory standard.

To run the NYCRR 500 report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **16** (New York Code Rules and Regulations 500).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run PCI DSS Report Card

The Payment Card Industry (PCI) Data Security Standard (DSS) was created by major credit card companies to combat the rise of security breaches against credit card account data. With strict enforcement of secure servers and network environments, the PCI DSS aims to keep credit cardholder data safe and secure. All organizations that process, store, or transmit credit card information must comply with PCI DSS.

Making sure your IBM i or iSeries server is compliant with PCI DSS begins with knowing what critical data resides on your server. If the system is used in any way for credit card transaction processing, PCI regulations need to be taken into account.

Most likely, a good place to start with your PCI compliance enforcement is tightening up user profile administration. Often, you will find unused user profiles, too many powerful profiles, and user profiles with default passwords. Getting these user profiles under control will help you ensure users only have access to one user profile account and that each user only has the authority needed to do their job.

To run the PCI DSS report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **1** (Payment Card Industry Data Security Standard: PCI DSS).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run Singapore Standard Report Card

The Singapore Technology Risk standards were created by the Monetary Authority of Singapore (MAS).

> **Note**: Go to MAS.gov.sa for additional information about this regulatory standard.

To run the Singapore Standard report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **11** (Technology Risk - Monetary Authority of Singapore).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation
Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Run SOX Report Card

The Sarbanes–Oxley (SOX) Act of 2002, also commonly called Sarbanes–Oxley, Sarbox or SOX, is a federal law in the United States that was enacted July 30, 2002. SOX mandates that executive management must individually certify the accuracy of financial information within an organization. In addition, much more severe penalties for fraudulent financial activity were implemented.

This regulation applies to any company which is publicly traded. There are also similar regulations in countries such as Canada, Japan, Germany, France, Italy, Australia, Israel, India, and South Africa.

Key provisions for SOX:

- 4.1 Sarbanes–Oxley Section 302: Disclosure controls
- 4.2 Sarbanes–Oxley Section 303: Improper influence on the conduct of audits
- 4.3 Sarbanes–Oxley Section 401: Disclosures in periodic reports (Off-balance sheet items)
- 4.4 Sarbanes–Oxley Section 404: Assessment of internal control
- 4.5 Sarbanes–Oxley 404 and smaller public companies
- 4.6 Sarbanes–Oxley Section 802: Criminal penalties for influencing US agency investigation/proper administration
- 4.7 Sarbanes–Oxley Section 906: Criminal penalties for CEO/CFO financial statement certification
- 4.8 Sarbanes–Oxley Section 1107: Criminal penalties for retaliation against whistleblowers

From a technical controls perspective, corporations are required to adhere to Section 404 which requires management and external auditors report on the adequacy of the company's internal control on financial reporting.

To run the SOX report card

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **10** (Regulation Report Cards).

3) Press **Enter**. The **Regulation Report Cards** interface is displayed.

4) At the **Selection or command** prompt, enter the **3** (Sarbanes Oxley Act: SOX).

5) Modify the run criteria and output option as necessary.

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

6) Press **Enter**.

Report Card Column Description

Column	Description
Regulation	Regulation ID
Category	Regulation category
Description	Description of regulation

Number of violations	Number of violations found
Pass/Fail Status	Status of your compliance to regulation
Report Link	Link to a detail description of passes and failures

See also

Working with Regulation Report Cards

Report History

This section describes how to work with the **Report History** feature. The report history allows you to display the list of reports previously generated.

- Working with Report and Report Card History
- Display Report History
- Display Report Details
- Re-display a Report Output
- Re-run Report

Working with Report and Report Card History

This section describes working with report and report card history:

- Display report history
- Display report details
- Re-display report output (only available for HTML, XML, and CSV output)
- Re-run report (using the same submittal parameters as the original report)

> **Note**: To work with report and report card history, access the **Report History** interface.

To access the Work with Report History interface

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

2) Press the **F20** (Report History) function key. The **Work with Report History** interface is displayed.

> **Tip**: For function keys higher than F12, you must use a combination of the **Shift** key and the appropriate function key. For example, to select F20, you must hold down the **Shift** key and F8.

See also

Report History

Display Report History

Use this task to do the following:

- Display List
- Sort List
- Move to Position in List
- Filter List

Display List

Use this task to display the list of reports previously generated.

To display report history

1) Access the **Main** menu.

2) Press the **F20** (Report History) function key. The **Report History** interface is displayed.

> **Tip**: The interface displays a list of the previously run reports in chronological order based on the **Run End Timestamp**.

Sort List

Use this task to sort the list or previously generated reports. The column on which the list is currently sorted appears in white text. For example, by default, the list is originally sorted by the **Run End Timestamp** column so that column heading initially appears in white text.

To sort report history using a column heading

1) Access the **Work with Report History** interface.

2) Place your cursor on a column heading (e.g., Report ID, Report Name, Collector ID, etc.).

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

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

Move to Position in List

Use this task to jump to a specific location within a sorted list. This is useful if you have a long list.

To move to a specific position within the report history

1) Access the **Work with Report History** interface.

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

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

4) Press **Enter**.

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

Filter List

Use this task to limit the what appears in the **Work with Report History** interface by defining a subset for filtering purposes.

To filter report history using a subset

1) Access the **Work with Report History** interface.

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

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

> **Tip**: For example, you can create a subset that limits the report history to only reports run in the last hour using the **Run End Date (From)** and **Run End Date (To)** fields.

4) Press **Enter**.

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

See also

Working with Report and Report Card History

Display Report Details

Use this task to display the run details (i.e., Job Name, Job User, Job Number, etc.) associated with a previous run report.

To display the report details

1) Access the **Work with Report History** interface.

2) Enter **5** (Run Details) in the **Opt** column for the desired report.

3) Press **Enter**.

See also

Working with Report and Report Card History

Re-display a Report Output

Use this task to view the results (output) of a previously run report.

> **Note**: The option is only available if the report was generated as HTML, XML, or CSV output. The system saves these output formats on the NetServer share.

To display the previously generated report output

1) Access the **Work with Report History** interface.

2) In the **Opt** column for the report you want to display, enter **8** (Last Run Results).

3) Press **Enter**.

See also

Working with Report and Report Card History

Configure the NetServer

Re-run Report

Use this task to re-run the report using the same submittal parameters as the original report.

> **Note**: This might be useful if you did not select HTML, XML, or CSV as the output format for the original report. The system saves these output format on the NetServer share.

To re-run the report using the same submittal parameters

1) Access the **Work with Report History** interface.

2) In the **Opt** column for the report you want to re-run, enter **7** (re-run).

3) Press **Enter**.

See also

Working with Report and Report Card History

Configure the NetServer

Report Outputs

This section describes how to work with **Report Outputs**. The report outputs are available in multiple formats (e.g., HTML, CSV, XML, etc.).

- Working with Report Outputs
- Display Report Failure Details
- Resolve Report Failures

Working with Report Outputs

You can produce reports and report cards in multiple output formats:

- HTML Output
- CVS Output
- XML Output

> **Tip:** HTML is the recommended output type because it takes advantage of the most user-friendly data layouts available. If you run a report from a client with an internet browser and have configured NetServer, the report should display automatically on your screen.

HTML Output

The following is an example of HTML output. This is the format produced when you select **HTML** as your output type.

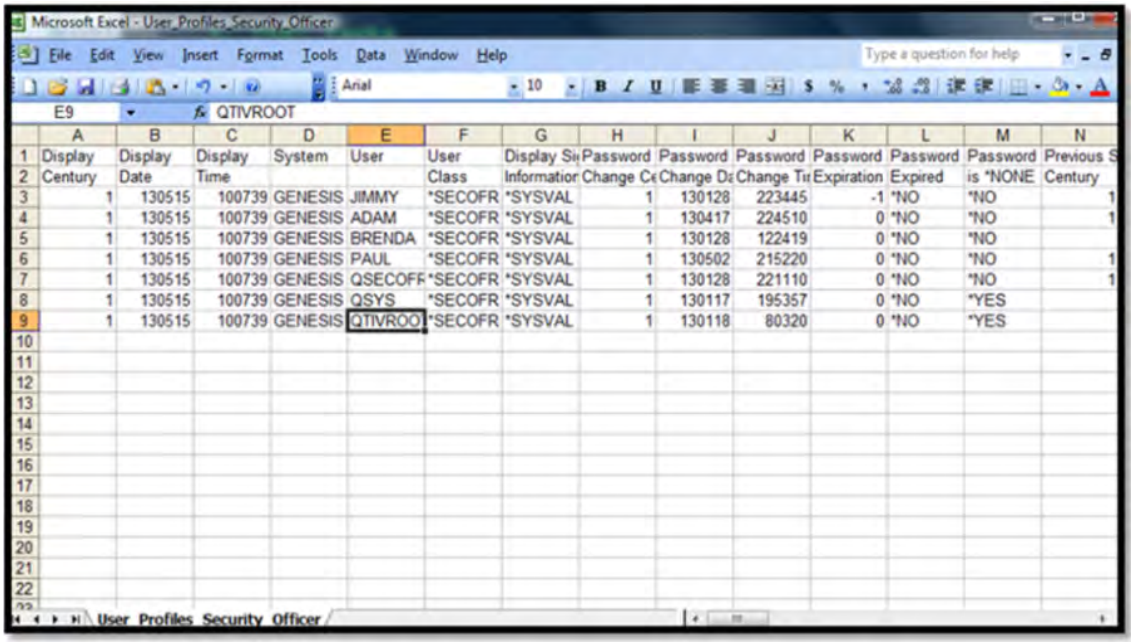
PCI DSS 3.2

Regulation	Category	Report Name	Number of Violations	Pass/Fail Status	Report Link	Help Link
1.1	Network	Network Connection Details	0	INFO	Detailed Report	
1.1.4	Network	Sockets-related Exit Points Not Secured	3	FAIL	Detailed Report	
1.1.4	Network	Unsecured Remote Server Exit Points	31	FAIL	Detailed Report	
1.1.5	Network	Secure Socket Connections	0	PASS	Detailed Report	
1.1.5	Network	Server Sessions Started or Ended	0	PASS	Detailed Report	

Figure: Sample HTML Output

CVS Output

The following is an example of CSV output. This is the format produced when you select **CSV** as your output type.

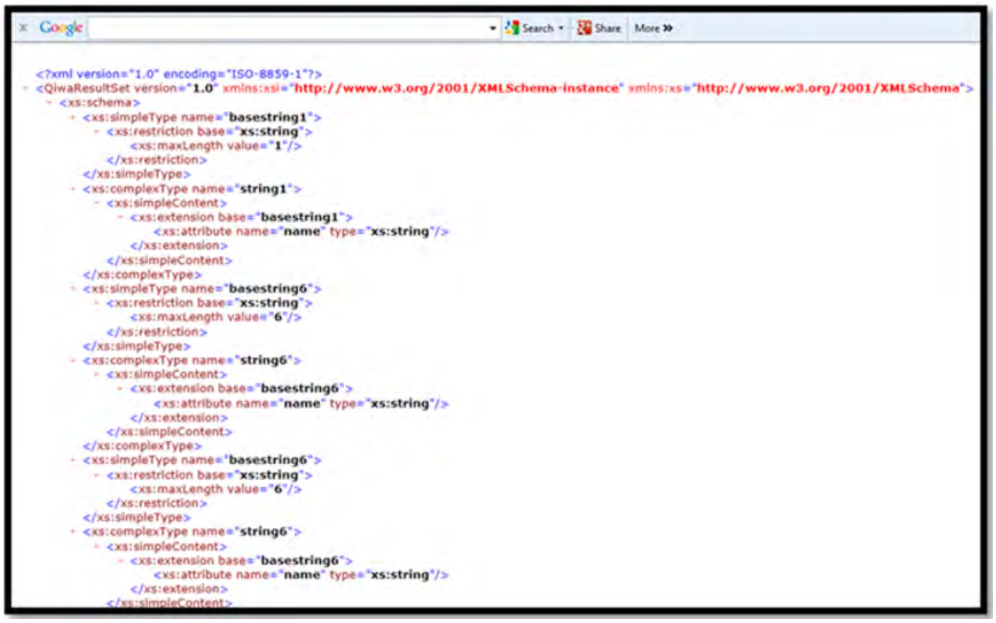


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Display	Display	Display	System	User	User	Display Si	Password	Password	Password	Password	Password	Password	Previous S
2	Century	Date	Time			Class	Informatior	Change Ce	Change Da	Change Ti	Expiration	Expired	is *NONE	Century
3	1	130515	100739	GENESIS	JIMMY	*SECOFR	*SYSVAL	1	130128	223445	-1	*NO	*NO	1
4	1	130515	100739	GENESIS	ADAM	*SECOFR	*SYSVAL	1	130417	224510	0	*NO	*NO	1
5	1	130515	100739	GENESIS	BRENDA	*SECOFR	*SYSVAL	1	130128	122419	0	*NO	*NO	
6	1	130515	100739	GENESIS	PAUL	*SECOFR	*SYSVAL	1	130502	215220	0	*NO	*NO	1
7	1	130515	100739	GENESIS	QSECOFF	*SECOFR	*SYSVAL	1	130128	221110	0	*NO	*NO	1
8	1	130515	100739	GENESIS	QSYS	*SECOFR	*SYSVAL	1	130117	195357	0	*NO	*YES	
9	1	130515	100739	GENESIS	QTIVROO	*SECOFR	*SYSVAL	1	130118	80320	0	*NO	*YES	

Figure: Sample CSV Output

XML Output

The following is an example of XML output. This is the format produced when you select **XML** as your output type.



```
<?xml version="1.0" encoding="ISO-8859-1"?>
- <QiwaResultSet version="1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  - <xs:schema>
    - <xs:simpleType name="basestring1">
      - <xs:restriction base="xs:string">
          <xs:maxLength value="1"/>
        </xs:restriction>
      </xs:simpleType>
    - <xs:complexType name="string1">
      - <xs:simpleContent>
        - <xs:extension base="basestring1">
            <xs:attribute name="name" type="xs:string"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    - <xs:simpleType name="basestring6">
      - <xs:restriction base="xs:string">
          <xs:maxLength value="6"/>
        </xs:restriction>
      </xs:simpleType>
    - <xs:complexType name="string6">
      - <xs:simpleContent>
        - <xs:extension base="basestring6">
            <xs:attribute name="name" type="xs:string"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    - <xs:simpleType name="basestring6">
      - <xs:restriction base="xs:string">
          <xs:maxLength value="6"/>
        </xs:restriction>
      </xs:simpleType>
    - <xs:complexType name="string6">
      - <xs:simpleContent>
        - <xs:extension base="basestring6">
            <xs:attribute name="name" type="xs:string"/>
          </xs:extension>
        </xs:simpleContent>
```

Figure: Sample XML Output

See also

Configure the NetServer

Display Report Failure Details

Use this task to view the report failure details.

To access the failure details

1) Run a report card and select HTML as the output format.

2) Once the HTML report displays, click the **Detailed Report** hyperlink in the **Report Link** column.

See also

Working with Report Outputs

Resolve Report Failures

Use this task to resolve report failures. Reports and report cards help you to identify areas within your system that are not properly secured. Once you are aware of these vulnerabilities, the next step is to rectify any issues found.

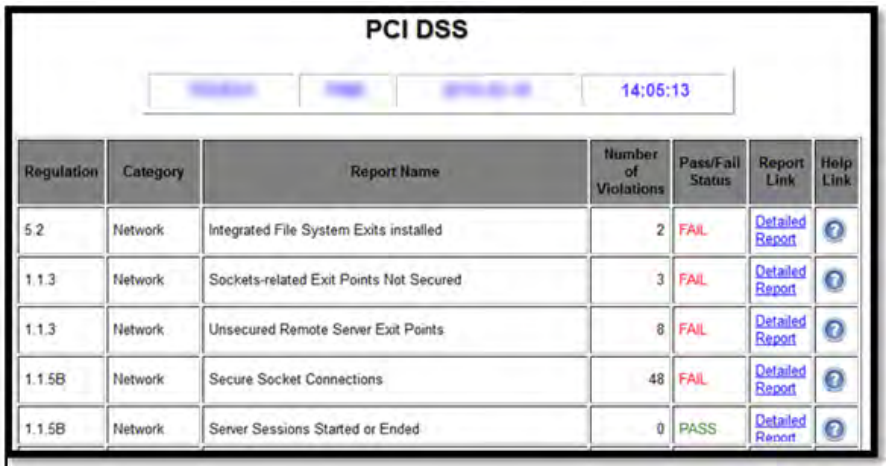
You can click on the Help icon on any report (HTML format) to get more information about the nature of the vulnerability.

It is in the best interest of your company to resolve any issues immediately to avoid serious security breaches. If you need further help and would like to discuss the findings, please contact support@trinityguard.com

To access the report help

1) Run a report card and select HTML as the output format.

2) Once the HTML report displays, click the **Help** icon to access online help specific to the report.



PCI DSS

14:05:13

Regulation	Category	Report Name	Number of Violations	Pass/Fail Status	Report Link	Help Link
5.2	Network	Integrated File System Exits installed	2	FAIL	Detailed Report	
1.1.3	Network	Sockets-related Exit Points Not Secured	3	FAIL	Detailed Report	
1.1.3	Network	Unsecured Remote Server Exit Points	8	FAIL	Detailed Report	
1.1.5B	Network	Secure Socket Connections	48	FAIL	Detailed Report	
1.1.5B	Network	Server Sessions Started or Ended	0	PASS	Detailed Report	

See also

Working with Report Outputs

Job Activity Monitor

This section describes how to work with the **Job Activity Monitor** (TGMJOBLOG). This feature allows you to monitor the job activity of interactive users and batch jobs running on your system. This type of monitoring is useful for auditing the activity of highly-privileged users who have access to sensitive information or who have the ability to run critical batch processing for sensitive jobs that ensure system integrity.

Summary information and detailed job log data about monitored jobs is available through an interactive screen. Both summary and detailed job activity reports are provided and have customizable run parameters to help optimize performance.

There are several types of objects activities you can monitor:

- Batch jobs (using subsystems)
- Interactive jobs (using commands)
- Activity Monitoring Rules
- User Groups

> **Note**: The job activity monitoring features are available through the **Job Activity Monitor** interface.

This section includes the following topics:

- Working with Job Activity Monitor
- Display Job Activities
- Manage Subsystems
- Manage Commands
- Manage Activity Monitor Rules
- Manage User Groups
- Archive Job Activity Data
- Run Job Activity Reports

To access the Job Activity Monitor interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the desired monitory activity.

5) Press **Enter**.

See also

TGAudit Introduction

Working with Job Activity Monitor

This section describes the task you can perform using the Job Activity Monitor:

- Display Job Activities
- Manage Subsystems
- Manage Commands
- Manage Activity Monitor Rules
- Manage User Groups
- Archive Job Activity Data
- Run Job Activity Reports

> **Note**: To work with the job activity monitor, access the **Job Activity Monitor** interface.

To access the Job Activity Monitor interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**. The **Job Activity Monitor** interface is displayed.

See also

Job Activity Monitor

Display Job Activities

Use this task to display job activity data. There are several ways to display job activities:

- Option 1. View Job Details via Job Activity Monitor
- Option 2. View Job Activity Summary Report
- Option 3. View Job Activity Details Report

> **Note**: To display job activities, access the **Job Activity Monitoring** interface.

To access the Job Activity Monitoring interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

Option 1. View Job Details via Job Activity Monitor

Use this task to view job details for a monitored job using the **Job Activity Monitor** interface.

Display Job Details for All Jobs

Use this task display the job detail for all jobs.

To view job details using the Job Activity Monitoring interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter **1** (Work with Job Activity).

5) Press **Enter**. The monitored jobs details are displayed in the **Work with Job Activity** screen.

Display Job Details for a Specific Job

Use this task display the job detail for a specific job.

To display the details for a specific job

1) Access the **Work with Job Activity** interface.

2) Enter **5** (Display) in the **Opt** column for the job you want to display.

> **Tip**: Once the job is displayed, you can use the **5** (Display MSG Data) to access messages associated with the job.

Sort Job Details

Use this task to sort the job details in ascending or descending order.

To sort job details

1) Access the **Work with Job Activity** interface.

2) Position your cursor on the column header you want to sort.

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

> ⚠ **Note**: The columns data is sorted in ascending order.

> ✓ **Tip**: To sort in descending order, press the **F10** function key a second time.

Filter Job Details

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

> ✓ **Tip**: Use the asterisk wildcard 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 the text (e.g., report*) to find list items that start with specific text.

– Add asterisks around the text (e.g., **report**) to find list items that contain specific text anywhere in the name.

To filter job details

1) Access the **Work with Job Activity** interface.

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

3) Modify the subset criteria as necessary.

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

4) Press **Enter** twice.

Option 2. View Job Activity Summary Report

Use this task to generate a job activity summary report.

To display job activity summary report

1) Access the **Job Activity Monitoring** interface.

2) At the **Selection or command** prompt, enter **2** (Job Activity Summary Report).

3) Press **Enter**.

4) Modify the search criteria and output option as necessary.

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

Option 3. View Job Activity Details Report

Use this task to generate a job activity details report.

To display job activity detail report

1) Access the **Job Activity Monitoring** interface.

2) At the **Selection or command** prompt, enter **3** (Job Activity Detail Report).

3) Press **Enter**.

4) Modify the run criteria and output option as necessary.

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

See also

Display Job Activities

Archive Job Activity Data

Working with Report Outputs

Manage Subsystems

Use this task to manage the subsystem on which you want to monitor the activity associated with batch jobs.

This topic describes the following tasks:

- Add Subsystem
- Edit Subsystem

To manage subsystems, access the **Work with Monitored Subsystems** interface.

To access the Work with Monitored Subsystems interface

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **12** (Work with Monitored Subsystems). The **Work with Monitored Subsystems** interface is displayed.

Add Subsystem

Use this task to add a subsystem you want to monitor.

To add a subsystem

1) Access the **Work with Monitored Subsystem** interface.

2) Press the **F6** (Add) function key on your keyboard.

3) Enter the following:

Field	Description
Subsystem name	Enter the subsystem you want to monitor
Subsystem library	Enter the library name associated with the subsystem
Log status	Enter ***ENABLED** to enable monitoring

4) Press **Enter**.

Edit Subsystem

Use this task to edit the details of a subsystem.

To edit a subsystem

1) Access the **Work with Activity Monitored Subsystems** interface.

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

3) Press **Enter**.

4) Modify the subsystem as necessary.

5) Press **Enter**.

See also

Working with Job Activity Monitor

Manage Commands

Use this task to manage the commands necessary to monitor interactive jobs.

This topic describes the following tasks:

- Add Command
- Edit Command

You can monitor one or more of the following commands.

- ENDJOB
- SIGNOFF
- ENDJOBABN
- ENDPASTHR

Tip: To ensure the most accurate monitoring of interactive user jobs, it's best to monitor all commands.

To manage commands, access the **Work with Monitored Commands** interface.

To access the Work with Monitored Commands interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **13** (Work with Monitored Commands).

Note: The **Work with Monitored Commands** interface is displayed.

Add Command

Use this task to add a command you want to monitor.

To add a command

1) Access the **Work with Monitored Commands** interface.

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

3) Enter the following:

Field	Description
Command Name	Enter the desired command (i.e., **ENDJOB, SIGNOFF, ENDJOBABN,** or **ENDPASTHR**)
Command Library	Enter the command library

4) Press **Enter**.

Edit Command

Use this task to edit the command details as necessary.

To edit a command

1) Access the **Work with Monitored Commands** interface.

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

3) Press **Enter**.

4) Modify the command as necessary.

5) Press **Enter**.

See also

Working with Job Activity Monitor

Manage Activity Monitor Rules

Use this task to manage activity monitor rules.

This topic describes the following tasks:

- Add Rule
- Edit Rule

Activity monitor rules identify the job activities you to monitor. You can apply a rule to a user or user group.

> **Note**: By default, a *PUBLIC rule exists that applies to all users. This default rule does not log any activity.

To manage activity monitor rules, access the **Work with Activity Monitor Rules** interface.

To access the Work with Activity Monitor Rules interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **10** (Work with Activity Monitor Rules). The **Work with Activity Monitor Rules** interface is displayed.

Add Rule

Use this task to add an activity monitor rule.

To add a rule

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

2) Press the **F6** (Add) function key on your keyboard.

3) Identify the user/group to which the rule applies.

4) Enter the following message logging details. These are the details you want to be assigned to the rule.

Field	Description
Level (0-4)	Specify the log level: 0 - No messages are logged 1 - Log messages with log level greater than or equal to 1 2 - Log messages with log level greater than or equal to 2 3 - Log messages with log level greater than or equal to 3 4 - Log messages with log level greater than or equal to 4
Severity (0-99)	Specify the severity level you want to be used in conjunction with the log level to determine which error messages are sent to the job log
Text	Specify the text you want to be sent to the job log

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

5) Press **Enter**.

Edit Rule

Use this task to edit an activity monitor rule.

To edit a rule

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

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

3) Press **Enter**.

4) Modify the rule as necessary.

5) Press **Enter**.

See also

Working with Job Activity Monitor

Manage User Groups

Use this task to create user groups.

This topic describes the following tasks:

- Add User Group
- Add Users to Group
- Edit User Group
- Delete User Group

User groups help ease rule management. When you create a user group, you can then add a rule for that user group name instead of having to create an individual rule for each user in the group.

To add a user group, access the **Work with User Groups** interface.

To access the Work with User Groups interface

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

2) At the **Selection or command** prompt, enter the **3** (Job Activity Monitor).

3) Press **Enter**.

4) At the **Selection or command** prompt, enter the **11** (Work with Groups). The **Work with User Groups** interface is displayed.

Add User Group

Use this task to add a user group.

To add a group

1) Access the **Work with User Group** interface.

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

3) Identify the user/group to which the rule applies.

4) Enter the message logging details specific to the rule.

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

5) Press **Enter**.

6) Enter the name and a description for the group.

> **Tip**: The group name must begin with a colon.

7) Press **Enter**.

Add Users to Group

Use this task to add a user group.

To add users to a group

Once the group is created, you can add users to that group.

1) Access the **Work with User Group** interface.
2) Enter **10** in the **Opt** column for the group you want to modify.
3) Press **Enter**.
4) Press the **F6** (Add) function key.
5) Enter the user's profile name and a description.
6) Press **Enter** twice.

> **Tip**: You can apply specific rules to both individuals and groups.

Edit User Group

Use this task to edit an existing user group.

To edit a user group

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

Delete User Group

Use this task to delete a user group.

To delete a user group

1) Access the **Work with User Group** interface.
2) In the **OPT** column for the desired group, enter **4** (Delete).
3) Ensure that you are deleting the correct group.
4) Press **Enter**.

See also

Working with Job Activity Monitor

Archive Job Activity Data

Use this task to archive job activity data.

> **Tip**: Since job activity data is very detailed, it can accumulate in large quantities very quickly. Therefore, you might need to manage your storage by archiving the data periodically.

To archive job activity data

1) Access the **Job Activity Monitoring Menu** interface.

2) At the **Selection or command** prompt, enter **20** (Job Activity Archival).

3) Press **Enter**.

Alternatively, at the IBM i command line, enter **TGJOBACTA**, and press the **F4** function key on your keyboard.

4) Modify the archival criteria as necessary.

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

See also

Working with Job Activity Monitor

Run Job Activity Reports

Use this task to generate job activity reports

- Access the Job Activity Monitor Menu Interface
- Run Job Activity Summary Reports
- Run Job Activity Detail Reports

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

Note: To work with job activity reports, access from the **Job Activity Monitor Menu** interface.

Access the Job Activity Monitor Menu Interface

To access the Job Activity Monitor Menu interface

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

2) At the **Selection or command** prompt, enter **4** (Job Activity Monitor).

3) Press **Enter**. The **Job Activity Monitor Menu** interface is displayed.

Run Job Activity Summary Reports

Use this task to produce a summary report of job activities.

To run the Job Activity Summary Reports

1) Access the **Job Activity Monitor Menu** interface.

2) At the **Selection or command** prompt, enter **2** (Job Activity Summary Report).

3) Press **Enter**. The **TG - Run Report (TGRPT)** interface is displayed.

4) Modify the report 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.

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

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

Note: See Job Activity Summary in the **TGAudit Report Reference Guide** for report details.

Run Job Activity Detail Reports

Use this task to produce a detailed report of job activities.

To run the Job Activity Details Report

1) Access the **Job Activity Monitor Menu** interface.

2) At the **Selection or command** prompt, enter **2** (Job Activity Details Report).

3) Press **Enter**. The **TG - Run Report (TGRPT)** interface is displayed.

4) Modify the report 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.

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

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

> **Note**: See Job Activity Details in the **TGAudit Report Reference Guide** for report details.

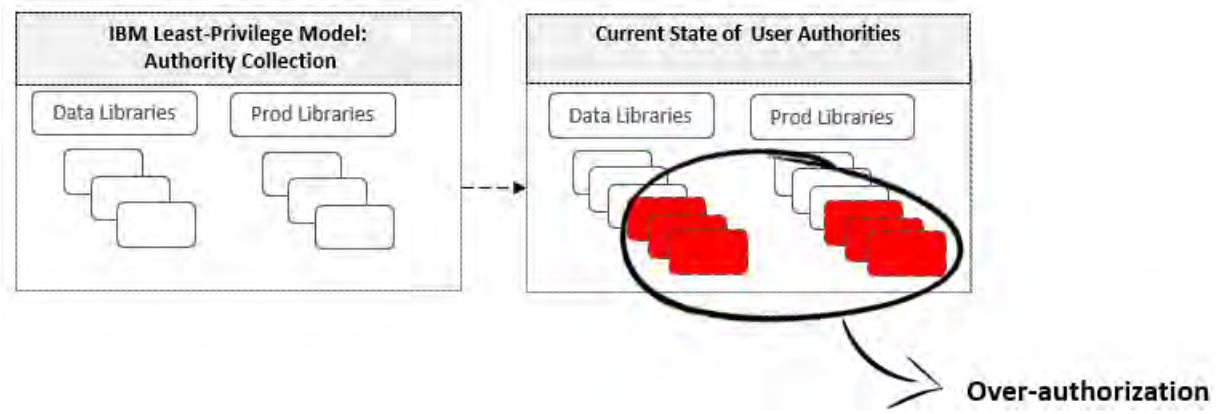
See also

Working with Job Activity Monitor

TGAudit Report Reference Guide

Authority Collection

This section describes how to work with the **Authority Collection** feature. When you enable authority collection, the system collects (for comparison purposes) the authorities defined by IBM's least-privileges model and the authorities current assigned to each user. You can use this information to determine the minimum authority requirements defined by IBM and determine if a user has been granted more authority than necessary. This helps you to eliminate unnecessary over-authorization.



> **Note**: The authority collection features are available through the **Authority Collection** interface.

This section includes the following topics:

- Working with Authority Collections
- Display Authority Collections
- Manage Authority Collection
- Run Authority Collection Reports

To access the Authority Collection interface

> **Important**: Authority collection is only available with OS IBM i 7.3. or higher. You will receive a warning message if your OS is not compatible with this feature.

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

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**.

4) Review the enrollment status of each user, and then make any necessary modifications.

See also

TGAudit Introduction

Working with Authority Collections

This section describes the task you can perform using the authority collections:

- Display Authority Collections
- Manage Authority Collection
- Run Authority Collection Reports

> **Note**: To work with authority collections, access the **Authority Collections** interface.

To access the Authority Collections interface

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

2) At the **Selection or command** prompt, enter the **4** (Authority Collection).

3) Press **Enter**. The **Work with Authority Collection Users** interface is displayed.

See also

Log Into TGAudit

Authority Collection

Display Authority Collections

Use this task to display the values on which the authority collections are based.

This topic describes the following tasks:

- Display Authority Collections by User
- Display Authority Collections by Object

Display Authority Collections by User

Use this task to display authority data by users.

> **Important**: You must have IBM 7.3 or higher to use this feature.

To display the authority collection details by user

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**. The **Authority Collection** interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Authority Collection by Users).

5) In the **Opt** column for the desired user, enter **5** (Display Collection Details)

6) Press **Enter**.

Field	Description
User Profile	Name of the user
Collection Active	Whether user authority data is collected: **YES** - Collection enabled (started) **NO** - Collection disabled (ended)
Repository Exists	Whether a repository exists for the storage of authority data: **YES** - Repository exits **NO** - Repository does not exist

Display Authority Collections by Object

Use this task to display authority data by object.

> **Important**: You must have IBM 7.4 or higher to use this feature.

To display the authority collection details by objects

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**. The **Authority Collection** interface is displayed.

4) At the **Selection or command** prompt, enter **2** (Work with Authority Collection by Object).

5) In the **Opt** column for the desired user, enter **5** (Display Collection Details)

6) Press **Enter**.

Field	Description
Object	Name of object
Collection Active	Whether object authority data is collected: **YES** - Collection enabled (started) **NO** - Collection disabled (ended)
Repository Exists	Whether a repository exists for the storage of authority data: **YES** - Repository exits **NO** - Repository does not exist

See also

Working with Authority Collections

Manage Authority Collection

Use this task to manage authority collections.

This topic describes the following tasks:

- Start Authority Collection using Main Menu
- Start Authority Collection using STRAUTCO Command
- End Authority Collection
- Delete Authority Collection

Start Authority Collection using Main Menu

Use this task to begin collecting authority collection information for a specified user using the **Main** menu.

> **Important**: You must have IBM 7.3 or higher installed to use this feature.

To start authority collection

1) Access the **Main** menu.

2) At the **Selection or command** prompt, enter **4** (Authority Collection):

3) Press **Enter**. The Authority Collection interface is displayed.

4) At the **Selection or command** prompt, enter **1** (Work with Authority Collection by Users).

5) Press the **F6** (Start Collection) function key on your keyboard.

6) Modify the criteria as necessary.

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

Start Authority Collection using STRAUTCO Command

Use this task to begin collecting authority collection information for a specified user using the STRAUTCOL command.

To start authority collection

1) At the IBM i command line, enter **STRAUTCOL**, and press the **F4** function key.

2) Modify the criteria as necessary.

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

End Authority Collection

Use this task to stop collecting authority information for a specified user.

> ⚠ **Important**: You must have IBM 7.3 or higher installed to use this feature.

To end the authority collection

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection).
3) Press **Enter**. The Authority Collection interface is displayed.
4) At the **Selection or command** prompt, enter **1** (Work with Authority Collection by Users).
5) In the **Opt** column for the desired user, enter **3** (End Collection).
6) Press **Enter**.

Delete Authority Collection

Use this task to delete the repository that was created for the user to collect authority information.

> ⚠ **Important**: The authority collection must be ended for the user before deleting the collection.

To delete the authority collection

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection).
3) Press **Enter**.
4) In the **Opt** column for the desired user, enter **4** (Delete Collection)
5) Press **Enter**.

See also

Working with Authority Collections

Run Authority Collection Reports

Use this task to generate the following reports:

- Access the Authority Collection Reports Interface
- Run Auth Collection For Users and Native Object Report
- Run Auth Collection For Users and IFS Report
- Run Auth Collection For Object Native Report
- Run Auth Collection For Object IFS Report
- Authority Collection Report (*ALL)

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

Note: To work with Authority Collection reports, access from the **Authority Collection Reports** interface.

Access the Authority Collection Reports Interface

To access the Inactive Sessions Reports interface

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

2) At the **Selection or command** prompt, enter **4** (Authority Collection).

3) Press **Enter**. The **Authority Collection** interface is displayed.

4) At the **Selection or command** prompt, enter **20** (Authority Collection Reports).

5) Press **Enter**. The **Authority Collection Reports** interface is displayed.

Run Auth Collection For Users and Native Object Report

Use this report to view the authority collections categorized by user.

Important: You must have IBM 7.3 or higher installed to use this feature.

To run the Authority Collection For Users and Native Object Report

1) Access the **Authority Collection Reports** interface.

2) At the **Selection or command** prompt, enter **1** (Auth Collection For Users and Native Object Report).

3) Press **Enter**. The **Run Report** interface is displayed.

4) 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.

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

> **Note**: See Authority Collection for Users and Native Object Report in the **TGAudit Report Reference Guide** for report details.

Run Auth Collection For Users and IFS Report

Use this report to view the authority collections categorized by user.

> **Important**: You must have IBM 7.3 or higher installed to use this feature.

To run the Authority Collection For Users and IFS Report

1) Access the **Authority Collection Reports** interface.

2) At the **Selection or command** prompt, enter **2** (Auth Collection For Users and IFS Report).

3) Press **Enter**. The **Run Report** interface is displayed.

4) 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.

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

> **Note**: See Authority Collection for Users and IFS Report in the **TGAudit Report Reference Guide** for report details.

Run Auth Collection For Object Native Report

Use this report to view the authority collections categorized by object.

> **Important**: You must have IBM 7.4 or higher installed to use this feature.

To run the Authority Collection For Object Native Report

1) Access the **Authority Collection Reports** interface.

2) At the **Selection or command** prompt, enter **3** (Auth Collection For Object Native Report).

3) Press **Enter**. The **Run Report** interface is displayed.

4) 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.

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

> **Note**: See Authority Collection for Object Native Report in the **TGAudit Report Reference Guide** for report details.

Run Auth Collection For Object IFS Report

Use this report to view the authority collections categorized by object.

> **Important**: You must have IBM 7.4 or higher installed to use this feature.

To run the Authority Collection For Object IFS Report

1) Access the **Authority Collection Reports** interface.

2) At the **Selection or command** prompt, enter **4** (Auth Collection For Object IFS Report).

3) Press **Enter**. The **Run Report** interface is displayed.

4) 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.

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

> **Note**: See Authority Collection for Object IFS Report in the **TGAudit Report Reference Guide** for report details.

Authority Collection Report (*ALL)

Use this report to view all authority collections.

To run the Authority Collection Report (*ALL)

1) Access the **Authority Collection Reports** interface.

2) At the **Selection or command** prompt, enter **5** (Authority Collection Report *ALL).

3) Press **Enter**. The **Run Report** interface is displayed.

4) 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.

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

> **Note**: See Authority Collection Report (*ALL) in the **TGAudit Report Reference Guide** for report details.

See also

Working with Authority Collections

TGAudit Report Reference Guide

Alerts

This section describes how to work with **Alerts**. Alerts are messages (notifications) triggered when specific criteria are met.

- Working with Alerts
- Manage Alerts

> **Note**: The alerting features are available through the **TGAudit Alert Defaults** interface.

To access the TGAudit Alert Defaults interface

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

2) At the Selection or command prompt, enter the **32** (Audit Configuration).

3) Press Enter. The **Audit Configuration** interface is displayed.

4) At the **Selection or command** prompt, enter the **10** (Alert Defaults). The **TGAudit Alert Defaults** interface is displayed.

See also

TGAudit Introduction

Working with Alerts

This section describes the alerting task(s) you can perform:

- Manage Alerts

> **Note**: To work with alerting, access the **TGAudit Alert Defaults** interface.

To access the TGAudit Alert Defaults interface

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

2) At the Selection or command prompt, enter the **32** (Audit Configuration).

3) Press Enter. The **Audit Configuration** interface is displayed.

4) At the **Selection or command** prompt, enter the **10** (Alert Defaults). The **TGAudit Alert Defaults** interface is displayed.

See also

Alerts

Manage Alerts

This section describes how to integrate TGDetect alerting in TGAudit. Both reports and report cards can trigger alerts.

> **Tip**: Set up alerts defaults before working with alerts.

- Enabling Alerting
- Configuring Alert Triggers for Reports
- Configuring Alert Triggers for Report Cards

Enabling Alerting

See Set Up Alert Defaults.

Configuring Alert Triggers for Reports

See Manage Custom Reports.

Configuring Alert Triggers for Report Cards

See Manage Custom Report Cards.

See also

Working with Alerts

Troubleshooting

This section provides resources to help you troubleshoot issues.

- TGAudit FAQs
- Error Messages

TGAudit FAQs

This section provides troubleshooting information you can use to resolve issues you might encounter.

- Why does my report have no data?

Why does my report have no data?

If you generate a report and it contains no data, you need to ensure that auditing has been enabled (see [Audit Configuration]).

Error Messages

Go here: IBM Errors

APPENDICES

- APPENDIX - Collectors
- APPENDIX - Revision History
  - Version 2.2 - TGAudit User Guide
  - Version 2.1 - TGAudit User Guide
- APPENDIX - TG Fix
- APPENDIX - TG Job Scheduler
- APPENDIX - TG Journal Cleanup
- APPENDIX - TG Management
- APPENDIX - TG Report Cleanup
- APPENDIX - TG Save and Restore

APPENDIX - Collectors

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

DATABASE ACCESS	Database File Access	N/A
DATABASE_AUDITING	Monitor Database changes	Network
DATABASE_CONTENT	Database Content	Configuration
DATABASE_OPERATIONS	Database Operations	N/A
DET_ACT_HISTORY	Detect Activity History	Network
DET_DEFAULTS	Detect Defaults	Configuration
DET_CMD_RULES	Command Monitor Rules	Configuration
DET_JRN_SEIM_RULES	Journal Monitor Rules for SEIM	Configuration
DET_JRNMON_ALERTS	Journal Monitor Alerts	Configuration
DET_JRNMON_RULES	Journal Monitor Rules	Configuration
DET_MON_MASTER	Monitor Master	Configuration
DET_MSQ_CMD_ALR	Message Queue and Command Alerts	Configuration
DET_MSQ_RULES	Message Queue Rules	Configuration
DET_SEIM_PROVIDERS	SEIM Providers	Configuration
DET_SNMP_TRP_PCKG	SNMP Trap Packages	Configuration
DEVICE_DESCRIPTION_APPC	Device Description APPC Information	Network
DEVICE_DESCRIPTION_DATA	Device Description Information	Network
DTBASE_OPERATIONS_JRN	Database Operations by Journal	N/A
EXIT_POINTS	Display Exit Point Data	Network
FIELD_AUTHORITY	Display Field Level Authorities	Object
IFS_ATTRIBUTES	Display the attributes for the IFS objects	Resource
IFS_AUTHORITIES	Display the public and private authorities associated with the object	Resource
IFS_CONTENT	IFS Content	Configuration
IFS_JOURNALING	Display extended journaling information for the IFS object	Resource
IFS_STATUS	Display status information about an IFS file	Resource
INCOMING_TRANSACTIONS	Incoming Transactions	Network
INACTIVITY_DISCONNECTS	Inactivity Disconnections	Configuration
ISL_CONFIGURATION_SETTINGS	ISL Configuration Settings	Network
ISL_DISCONNECT_OPTIONS	ISL Disconnect Options	Network
ISL_RULES	ISL Inclusion Exclusion Rules	Network

JOB_ACTIVITY_DETAILS	Job Activity Details	Log
JOB_ACTIVITY_SUMMARY	Job Activity Summary	Log
JOB_DESCRIPTIONS	Job Description Data	Configuration
JOURNAL_AD	Object Auditing Attribute Changes	Configuration
JOURNAL_AF	Authority Failures	Profile
JOURNAL_AP	Programs that Adopt Authority were Executed	Configuration
JOURNAL_AU	EIM Attribute Changes	Configuration
JOURNAL_AX	Row and Column Access Control	Resource
JOURNAL_CA	Authorization List or Object Authority Changes	Profile
JOURNAL_CD	Commands Executed	Resource
JOURNAL_CO	Create Operations	Resource
JOURNAL_CP	User Profile Changes	Configuration
JOURNAL_CQ	Change Request Descriptor Changes	Configuration
JOURNAL_CU	Cluster Operation	Network
JOURNAL_CV	Connection Verification	Profile
JOURNAL_CY	Cryptographic Configuration Changes	Configuration
JOURNAL_DI	LDAP Operations	Resource
JOURNAL_DO	Delete Operations	Resource
JOURNAL_DS	Changes to Service Tools Profiles	Profile
JOURNAL_EV	Environment Variable Changes	Profile
JOURNAL_GR	Exit Point Maintenance Operations	Resource
JOURNAL_GS	Socket Descriptor Details	Resource
JOURNAL_IM	Intrusion Monitor Events	Network
JOURNAL_IP	Inter-process Communication Events	Network
JOURNAL_IR	Actions to IP Rules	Network
JOURNAL_IS	Internet Security Management Events	Network
JOURNAL_JD	Job Descriptions – USER Parameter Changes	Resource
JOURNAL_JS	Job Changes	Resource
JOURNAL_KF	Key Ring File Changes	Configuration
JOURNAL_LD	Directory Link, Unlink, and Search Operations	Resource
JOURNAL_M0	Db2 Mirror Setup Tools	Resource

JOURNAL_M6	Db2 Mirror Communication Services	Resource
JOURNAL_M7	Db2 Mirror Replication Services	Resource
JOURNAL_M8	Db2 Mirror Product Services	Resource
JOURNAL_M9	Db2 Mirror Replication State	Resource
JOURNAL_ML	OfficeVision Mail Services Actions	Configuration
JOURNAL_NA	Network Attribute Changes	Profile
JOURNAL_ND	Directory Search Violations	Resource
JOURNAL_NE	APPN Endpoint Filter Violations	Network
JOURNAL_O1	Single Optical Object Accesses	Resource
JOURNAL_O2	Dual Optical Object Accesses	Resource
JOURNAL_O3	Optical Volume Accesses	Resource
JOURNAL_OM	Object Management Changes	Resource
JOURNAL_OR	Objects Restored	Resource
JOURNAL_OW	Object Ownership Changes	Resource
JOURNAL_PA	Program Changes to Adopt Owner Authority	Configuration
JOURNAL_PF	PTF Operations	Resource
JOURNAL_PG	Primary Group Changes	Resource
JOURNAL_PO	Printer Output Changes	Resource
JOURNAL_PS	Swap Profile Events	Configuration
JOURNAL_PU	PTF Object Changes	Profile
JOURNAL_PW	Invalid Sign-on Attempts	Profile
JOURNAL_RA	Authority Changes to Restored Objects	Configuration
JOURNAL_RJ	Job Descriptions that Contain User Profile Names were Restored	Configuration
JOURNAL_RO	Ownership Changes for Restored Objects	Profile
JOURNAL_RP	Programs Restored that Adopt Owner Authority	Configuration
JOURNAL_RQ	Change Request Descriptors Restored	Resource
JOURNAL_RU	Authority Restored for User Profiles	Profile
JOURNAL_RZ	Primary Group Changes for Restored Objects	Configuration
JOURNAL_SD	System Directory Changes	Resource
JOURNAL_SE	Subsystem Routing Entry Changes	Configuration

JOURNAL_SF	Spooled File Actions	Resource
JOURNAL_SG	Asynchronous Signals Processed	Network
JOURNAL_SK	Secure Socket Connections	Network
JOURNAL_SM	Systems Management Changes	Configuration
JOURNAL_SO	Server Security User Information Actions	Configuration
JOURNAL_ST	Service Tools Actions	Configuration
JOURNAL_SV	System Values Changes	Configuration
JOURNAL_VA	Access Control List Changes	Configuration
JOURNAL_VC	Connections Started, Ended, or Rejected	Network
JOURNAL_VF	Close Operations on Server Files	Resource
JOURNAL_VL	Exceeded Account Limit Events	Profile
JOURNAL_VN	Network Log On and Off Events	Configuration
JOURNAL_VO	Actions on Validation Lists	Resource
JOURNAL_VP	Network Password Errors	Profile
JOURNAL_VR	Network Resource Accesses	Resource
JOURNAL_VS	Server Sessions Started or Ended	Network
JOURNAL_VU	Network Profile Changes	Profile
JOURNAL_VV	Service Status Change Events	Network
JOURNAL_X0	Network Authentication Events	Network
JOURNAL_X1	Identity Token Events	Profile
JOURNAL_XD	Directory Server Extensions	Profile
JOURNAL_YC	DLO Object Changes	Resource
JOURNAL_YR	DLO Object Reads	Resource
JOURNAL_ZC	Object Changes	Resource
JOURNAL_ZR	Object Reads	Resource
KEYSTORE_DATA	KeyStore	Configuration
LIBRARY_STAT	Library Statistics	Resources
LINE_DESCRIPTION_DATA	Line Description Information	Configuration
MESSAGE_QUEUE	Message Queue Details	Configuration
MESSAGE_QUEUE_DATA	Message Queue Data	Configuration
NETWORK_ATTRIBUTES	Network Attribute Information	Network

NETWORK_CONNECTIONS	Network Connections Ipv4 and Ipv6	Network
NETWORK_EXIT_CONFIG	Exit Point Configuration Report	Network
NETWORK_INTERFACE_IPV4	Network Interface Data Ipv4	Network
NETWORK_INTERFACE_IPV6	Network Interface Data Ipv6	Network
NETWORK_ROUTE_IPV4	Network Route Data Ipv4	Network
NETWORK_ROUTE_IPV6	Network Route Data Ipv6	Network
NETWORK_SERVER_DESCRIPTIONS	Network Server Description Data	Network
NETWORK_SVR_ENCRYPT_STATUS	Network Server Encryption Status	Network
NETWORK_TCPIP_IPV4	TCP/IP Ipv4 Stack Attributes/Remote Exit Rule	Network
NETWORK_TCPIP_IPV6	TCP/IP Ipv6 Stack Attributes/Remote Exit Rule	Network
NETWORK_TRANS_CENTRAL	Central Server Transactions	Network
NETWORK_TRANS_COMMAND	Remote Command Transactions	Network
NETWORK_TRANS_DATABASE	Remote Exit Rules	Network
NETWORK_TRANS_DATAQ	Remote Exit Rules	Network
NETWORK_TRANS_DDM	Remote Exit Rules	Network
NETWORK_TRANS_FILE	Remote Exit Rules	Network
NETWORK_TRANS_FTP_REXEC	Remote Exit Rules	Network
NETWORK_TRANS_PRINTER	Remote Exit Rules	Network
NETWORK_TRANS_SHOWCASE	Network Trans Showcase	Network
NETWORK_TRANS_SIGNON	Remote Exit Rules	Network
NETWORK_TRANS_TELNET	Remote Exit Rules	Network
OBJECT_AUTHORITY	Display Object Authority	Resource
OBJECT_DETAILS	Display Object Details	Resource
OBJECT_STAT	Object/File Statistics	Resource
OUTPUT_QUEUE	Output Queue Information	Configuration
PRODUCT_INFO	Basic Information about a software product	Configuration
PROFILE_COMPLIANCE	Profile Compliance Data	Profile
PROFILE_INACTIVITY_SETTINGS	Profile Inactivity Settings	Profile
PROFILE_MANAGER_DEFAULTS	Profile Manager Defaults	Profile
PROGRAM_ADOPT	Programs that Adopt Authority	Resource

PROGRAM_REFERENCE_DATA	Program Reference Data	Resource
PTF_DATA	Program Temporary Fix Data	Configuration
QHST_MSG_INFO	QHST History Log Information	Configuration
QSYS2.ACTIVE_JOB_INFO	Active job information	Configuration
QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User access	Configuration
QSYS2.FUNCTION_INFO	Function usage identifiers	Configuration
QSYS2.FUNCTION_USAGE	Function usage configuration details.	Configuration
QSYS2.GROUP_PTF_INFO	Group PTFs Information	Configuration
QSYS2.JOURNAL_INFO	Journal and remote journal information	Configuration
QSYS2.LICENSE_INFO	Products license information.	Configuration
QSYS2.MEDIA_LIBRARY_INFO	Media Library Status details	Configuration
QSYS2.MEMORY_POOL	Memory pool details	Configuration
QSYS2.MEMORY_POOL_INFO	Active memory pools	Configuration
QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 network connection details.	Configuration
QSYS2.OBJECT_LOCK_INFO	Object lock information	Configuration
QSYS2. OUTPUT_QUEUE_ENTRIES	Spooled file in output queue	Configuration
QSYS2.RECORD_LOCK_INFO	Record lock information	Configuration
QSYS2.REPLY_LIST_INFO	Current job's reply list entry information	Configuration
QSYS2.SCHEDULED_JOB_INFO	Job Schedule Entry information	Configuration
QSYS2.SERVER_SBS_ROUTING	Alternate subsystem configurations	Configuration
QSYS2.SYSCONTROLS	Permissions or column mask defined	Configuration
QSYS2.SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
QSYS2.SYSDISKSTAT	Disk Information	Configuration
QSYS2.SYSTEM_STATUS_INFO	Partition information	Configuration
QSYS2.SYSTMPSTG	IBM i temporary storage pool detail	Configuration
QSYS2.USER_INFO	User Profile Information	Configuration
QSYS2.USER_STORAGE	Storage usage by user profile	Configuration
REMOTE_TRAN_SUMMARY_BY_SERVER	Remote Summary Server	Network
REMOTE_TRAN_SUMMARY_BY_USER	Remote Summary User	Network

RSC_MGR_COMPLIANCE_DATA	Resource Manager Authority Out of compliance data	Network
RSC_MGR_CONFIG	Resource Manager Configuration	Network
RSC_MGR_SCHEMA_DETAILS	Resource Manager Authority Schema Details	Network
RSC_MGR_SCHEMA_HEADER	Resource Manager Authority Schema Header	Network
SENSITIVE_DATABASE_CONTENT	Sensitive Database Content	Profile
SERVICE_TOOL_SECURITY_ATTR	Service Tool Security Attributes	Profile
SERVICE_TOOL_USERS	Service Tool User Data	Profile
SOCKET_SUMMARY_BY_SERVER	Socket Summary by Server	Network
SOCKET_SUMMARY_BY_USER	Socket Summart by User	Network
SOCKET_TRAN_RULES	Socket Rules	Network
SOCKET_TRANSACTIONS	Socket Transactions	Network
SOFTWARE_RESOURCES	Installed Software Resources Data	Configuration
SUBSYSTEM_AUTOSTART	Subsystem Autostart Jobs	Configuration
SUBSYSTEM_COMMUNICATIONS	Subsystem Communication Entries	Configuration
SUBSYSTEM_INFORMATION	Subsystem Information Details	Configuration
SUBSYSTEM_JOB_QUEUE	Subsystem Job Queue	Configuration
SUBSYSTEM_POOL_DATA	Subsystem Pool Data	Configuration
SUBSYSTEM_PRESTART	Subsystem Prestart Jobs	Configuration
SUBSYSTEM_REMOTE	Subsystem Remote Entries	Configuration
SUBSYSTEM_ROUTING	Subsystem Routing Entries	Configuration
SUBSYSTEM_WORKSTATION_NAMES	Subsystem Workstation Names	Configuration
SUBSYSTEM_WORKSTATION_TYPES	Subsystem Workstation Types	Configuration
SYSCOLAUTH	Privileges granted on a column	Configuration
SYSCONTROLS	Permission or column mask defined	Configuration
SYSCONTROLSDEP	Dependencies of row permissions and column masks	Configuration
SYSCONTROLSDEP	Privileges granted on a row	Configuration
SYSFIELDS	Columns with field procedures	Configuration
SYSPACKAGEAUTH	Privileges granted on a package	Configuration
SYSPROGRAMSTAT	Program, service program, and module with SQL statements	Configuration

SYSROUTINEAUTH	Privileges granted on a routine	Configuration
SYSSCHEMAAUTH	Privileges granted on a schema	Configuration
SYSSEQUENCEAUTH	Privileges granted on a sequence	Configuration
SYSTABAUTH	Privileges granted on a table or view	Configuration
SYSTABLESTAT	Table statistics include all partitions and members	Configuration
SYSTEM_VALUES	Display System Value Data	System
SYSTOOLS. GROUP_PTF_CURRENCY	PTF Groups installed per IBM Recommendations	Configuration
SYSTOOLS. GROUP_PTF_DETAILS	PTFs within PTF Groups installed per IBM Recommendations	Configuration
SYSUDTAUTH	Privileges granted on a type	Configuration
SYSVARIABLEAUTH	Privileges granted on a global variable	Configuration
SYSXSROBJECTAUTH	Privileges granted on an XML schema	Configuration
TGMOBJINF	Object Information	Resource
TG_NETWORK_GROUPS	TG Network Groups	Network
TG_OBJECT_GROUPS	TG Object Groups	Network
TG_OPERATION_GROUPS	TG Operation Groups	Network
TG_USER_GROUPS	TG User Groups	Network
USER_OBJECT_AUTHORITIES	User Profile Object Authorities	Profile
USER_PRF_VIA_BLUEPRINT	User Profile via Blueprint	Profile
USER_PROFILE_ACTIVITY	User Profile Activity	Profile
USER_PROFILE_ARCHIVE	User Profile Archive	Profile
USER_PROFILE_EXCLUSIONS	User Profile Exclusions	Profile
USER_PROFILES	Display User Profile Data	Profile

APPENDIX - Revision History

This section includes enhancement by version.

- Version 2.2 - TGAudit User Guide
- Version 2.1 - TGAudit User Guide

Version 2.2 - TGAudit User Guide

This release includes the following:

Alert Defaults

You can now set up alerts defaults.

Job Scheduler

You can now set up a job scheduler.

Collectors

The following new collectors are now available:

- AUTHORITY_COL_ALI
- AUTHORITY_COL_IFS
- AUTHORITY_COL_OBJECT
- DATABASE_ACCESS
- DATABASE_OPERATIONS
- DTBASE_OPERATIONS_JRN
- QHST_MSG_INFO
- SENSITIVE_DATABASE_CONTENT

Authority Collection Reports

The following Authority Collection reports are now available:

- Authority Collection for Object IFS Report
- Authority Collection for Object Native Report
- Authority Collection Report (*ALL)

Configuration Reports

The following new Configuration reports are now available for use:

- QHST Message Information
- QHST Messages with Severity Greater Than 40

Data Level Reports

The following Data Level reports are now available.

- Database Access
- Database Operations
- Database Operations by Journal

Resource Reports

The following Resource reports are now available:

- Changed Data Files in Last 30 Days
- Damages Objects

- Files Not Used in the Last 30 Days
- Journaled Files
- New Data Files in Last 30 Days
- New Library in Last 30 Days
- New Objects in the Last 30 Days
- Object Source
- Objects Changed in the Last 30 Days
- Objects Created in the Last 30 Days
- Objects Larger than 100MB
- Objects Owned by QSECOFR
- Objects Used in the Last 30 Days
- Restored Objects in the Last 30 Days
- Source Changes in Last 30 Days
- Unsaved Objects in the Last 30 Days

Version 2.1 - TGAudit User Guide

This release includes the following:

Alerts

Alerting is now available in TG Audit. See the following topics for details:

- Set Up Alert Defaults
- Manage Alerts

Collectors

The following new collectors are now available for use:

- IFS_CONTENT
- DATABASE_CONTENT
- NETWORK_TRANS_SHOWCASE

> **Note**: See APPENDIX - Collectors for a complete list of available collectors.

Reports

The following reports are now available for use:

- Database Content
- Cross Reference Physical File
- Schedule Master File
- Integrated File System Content
- TGAudit Report Configuration
- TGCentral Agent Configuration
- Network Transaction Showcase Report

> **Note**: See Run Reports for instruction on how to run a report.

> **Tip**: See the **TG Audit Report Reference Guide** for information about individual reports.

New Report Cards

- AICPA GAPP
- COBIT 5 Framework
- IRS_Publication 1075
- NERC Critical Infrastructure Protection V5
- Cloud Security Alliance
- Technology Risk - Monetary Authority of Singapore

- FFIEC Cybersecurity Assessment Tool
- ITIL Key Performance Indicator
- Nevada Gaming Minimum Internal Control Standards
- New York Code Rules and Regulations 500

Note: See the TGAudit Report Reference for documentation on individual report cards.

APPENDIX - TG Fix

The **TG Fix** tool allows you to install fixes via the TG menu quickly and easily. This feature also includes verification features that ensure the fix is installed properly.

See also

Working with TG Fix

APPENDIX - TG Job Scheduler

APPENDIX - TG Journal Cleanup

The **TG Journal Cleanup** (TGJRNCLEAN) tool is a command-line tool that allows you to manage journal receiver data.

Journaling is widely used on IBM i servers to keep track of database changes as well as system and security level audit information. Journal data cannot be altered or corrupted. Therefore, it is very useful for forensic analysis and makes IBM i the best platform for security. With all these journaling capabilities, cleaning up old journal data becomes a critical task for the system administrator or storage issues could result.

> ⚠ **Important**: Before using this tool, review your data retention policy and make a backup of the receivers for later retrieval. In case of a security incident investigation, old receiver data is required for forensic analysis.

See also

Journal Cleanup Tool

Journaling Concepts

Journal Management

APPENDIX - TG Management

The **TG Management** tool allows you to configure TG product administrative elements (e.g., licensing, user authorization, report output formats, etc.).

See also

Working with TG Management

APPENDIX - TG Report Cleanup

The **TG Report Cleanup** (TGRPTCLEAN) tool is a command-line tool that allows you to manage HTML report data stored in the IFS.

> **Tip**: You can purge report data automatically on a scheduled basis using this tool.

See also

Working with TGRPTCLEAN

APPENDIX - TG Save and Restore

The **TG Save and Restore** tool allows you to save the configuration of a specific instance of TGSecure or TGAudit. Once you save a configuration, you can then use that saved configuration file to do the following:

- Create a back-up (archive) of the current configuration to be used later to restore the configuration of an agent (server)
- Create multiple instances with identical configuration

A saved file stores the configuration for the following:

- Calendars
- Entitlement
- Groups
- Networks
- Reports
- Rules (i.e., Socket Rules, Exit Rules, etc.)

See also

Working with the TG Save and Restore