NetIQ Security Solutions for IBM i
TGAudit 1.7
User Guide
Revised Februrary 2018

Legal Notice

Table of Contents

What's New in Version 1.7
This release of TGAudit includes performance improvements and a new feature called Save/Restore Configuration.

What's New in Version 1.6
This release of TGAudit includes minor bugs fixes, but no new features.

What's New in Version 1.5
New Features
- You can now access feature-specific online help for any TGAudit green screen by clicking the **F1** function key.
- You can now access command-specific (e.g., F4, F10, etc) online help for any TGAudit command by clicking the **F1** function key.

Enhancements

- The Work with Reports interface has been enhanced to include a report wizard that walks you through the process of adding custom reports.
- The Work with Reports interface has been enhanced to allow you to sort, filter, and jump to a specific location within the list of available reports.
- The Work with Report History interface has been enhanced to allow you to sort, filter, and jump to a specific location within a list of previously run reports.

Report Cards

The **PCI 3.2** built-in report card is now available. This report card addresses the 3.2 updates for the Payment Card Industry (PCI) data security regulation.

Reports

The **Programs that Adopt Authority** report is now available as a build-in regulatory report. See IBM.com (https://www.ibm.com/support) for details regarding the adopt authority security feature.

Note: Refer the **Report Reference Guide** (PDF file) for details about any built-in regulatory report, or run the report and select HTML as the output format, and then click the Help  icon to access online help specific to the report.

Collectors

No new collectors were added in this release.

1. Introduction

1.1. Product Overview

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.

See also:

Benefits

Features

1.2. 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

1.3. 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 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

2. Setup

2.1. Audit Configuration

This section walks you through the steps necessary to configure auditing:

- Set up system auditing
- Set up object auditing
- Set up IFS auditing
- Set up database journaling
- Set up data area journaling
- Set up range of journal receivers for reports
- Set up journal receiver cleanup
- Set up report data cleanup

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 manage audit configuration details, 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**.

Note: The **TGAudit - Main** menu is displayed.

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

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

2.2. 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).

Note: 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).

2.3. 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).

Note: 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	Activity you want to monitor (e.g., who has viewed object, who has changed 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 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.

2.4. 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).

Note: 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.

2.5. 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).

Note: The **Start Journal Object** interface 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 **Data Area Changes** reports available in the **Data Level Reports** menu.

2.6. 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).

Note: 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.

2.7. Set Up Journal Receiver Cleanup

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) Enter the criteria you want to use to perform the receiver cleanup.

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.

2.8. Set Up Report Data Cleanup

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

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) Enter the criteria you want to use to perform the report data cleanup.

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.

3. Using TGAudit

3.1. Getting Started Using TGAudit

This section describes how to perform the following basic tasks:

- Work with Reports
- Work with Report Cards
- Work with Report History
- Work with Report Outputs

3.2. Working with Reports

3.2.1. Working with Reports

This section describes working with built-in reports.

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

To access the Work with Reports interface

1) Access the **TG Main** menu.
2) At the **Selection or command** prompt, enter **30** (Work with Reports).
3) Press **Enter**.

See also:

Custom Reports

3.2.2. Display List of Reports

Use this task to do the following:

- Display the list
- Sort the list
- Move to a specific location within the list
- Filter the list

3.2.2.1. 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**.

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

3.2.2.2. 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.

3.2.2.3. 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**.

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

3.2.2.4. 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**.

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

3.2.3. Run Reports Using Main Menu

Use this task to run a report using the **Main** menu, which allows you to run a report immediately.

To run a report using the Main menu

1) Access the **Main** menu.
2) At the **Selection or command** prompt, enter the category (**1**, **2**, **3**, **4**) of report you want to run:

– **1**. Security and Configuration Reports
– **2**. Data Level Reports
– **3**. Job Activity Monitor

– **4**. Authority Collection

3) Press **Enter**.
4) At the **Selection or command** prompt, enter the number of the report you want to run.
5) Press **Enter**.
6) Make any necessary subcategory selections until you reach the **TG - Run Report (TGRPT)** interface.
7) Modify the run 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.

8) Enter the desired output type in the **Report output type** field.
9) Press **Enter**.

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

See also: Working with Report Outputs

3.2.4. Run Reports

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

To run a report using the Work with Reports interface

1) Access the **TG 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	***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. See Create Reports for additional information about setting up run-time collector defaults.
Reload 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 data source collection

Field	Description
Report output type	Enter the desired report output format (*HTML, *PRINT, etc.)
Run interactively?	***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**.

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

3.2.5. Run Reports Using TGRPT Command

Use this task to run a report using the **TGRPT** interface, which allows you to schedule the running of a report using command line access.

To run a report using the TGRPT command

1) Access the **Main** menu.
2) Press the **F18** (Run Report) function key.

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 F18, you must hold down the **Shift** key and F6.

3) Enter the desired collector in the **Collector ID** field.

Tip: Press **F4** (Prompt) to see a list of valid options.

4) Press **Enter**.
5) Enter the desired report in the **Report ID** field.
6) Press **Enter**.
7) Enter the desired output type in the **Report output type** field.
8) Press **Enter**.

Tip: If you choose HTML, XML, or CSV as your report output, but a report does not display, then ensure that the NetServer has been configured for HTML, CSV, and XML outputs.

See also: Configure the NetServer

3.3. Working with Report Cards

3.3.1. Working with Report Cards

There are several ways to work with report cards:

- Run reports using the **Work with Report Cards** interface, which allows you to configure (i.e., edit, copy, etc.) report card
- Run reports using the **TGAudit** menu options, which allows you to run a report card immediately
- Run reports using the **TGCARD** command interface, which allows you to schedule the running of a report card using command line access

To access the Work with Report Cards interface

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **31** (Work with Report Cards).
3) Press **Enter**.

See also: Custom Report Cards

3.3.2. Run Report Card using Main Menu

Use this task to run a report card using the **Main** menu, which allows you to run a report card immediately.

To run a report cards using the Main menu

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **10** (Regulation Report Cards).
3) Press **Enter**.
4) At the **Selection or command** prompt, enter the number of the report card you want to 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

3.3.3. Run Report Card using Work with Report Cards Interface

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 **TGAudit** 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

3.3.4. Run Report Card using TGCARD Command

Use this task to run a report card using the **TGCARD** command, which allows you to schedule the running of a report card using command line access.

To run a report using the TGCARD command

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

2) Press the **F19** (Run Report Card) function key.

Alternatively, at the IBM i command line, enter **TGCARD**, and press the **F4** function key.

3) Enter the desired report card in the **Report Card ID** field.

Tip: Press **F4** (Prompt) to see a list of available report cards.

4) Press **Enter**.
5) Modify the criteria and output option for the report card 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

3.4. Working with Report History

3.4.1. Working with Report and Report Card History

There are several ways to work with report 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

To access the Work with Report History interface

1) Access the **TGAudit Main** menu.
2) Press the **F20** (Report History) function key.

Note: The **Report History** interface is displayed.

3.4.2. Display Report History

Use this task to do the following:

- Display report history
- Sort report history
- Move to a specific location within report history
- Filter report history

3.4.2.1. Display List

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

To display report history

1) Access the **TGAudit Main** menu.
2) Press the **F20** (Report History) function key.

Note: 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**.

3.4.2.2. 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.

3.4.2.3. Move to Position in List

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

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.

3.4.2.4. 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.

3.4.3. 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**.

3.4.4. 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: Configure the NetServer

3.4.5. 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: Configure the NetServer

3.5. Working with Report Outputs

3.5.1. Working with Report Outputs

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

- HTML
- CSV (Excel)
- XML
- Spooled File
- Output File

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.

See also: Configure the NetServer

3.5.1.1. HTML Output

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

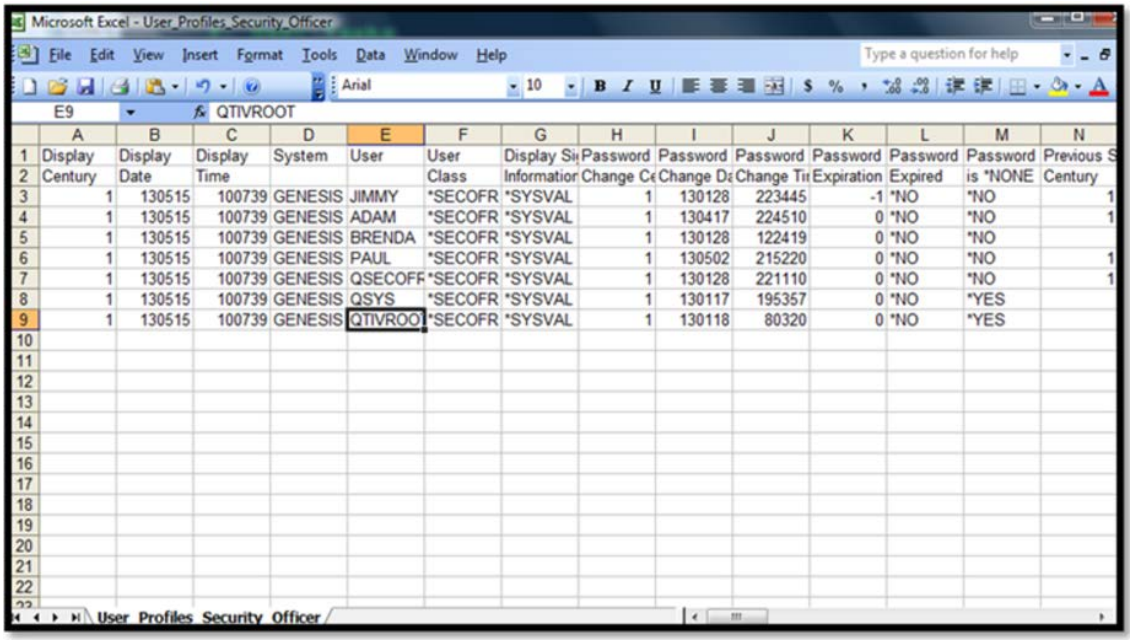
PCI DSS 3.2

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

3.5.1.2. 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	Information	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	QTIVROOT	*SECOFR	*SYSVAL	1	130118	80320	0	*NO	*YES	

Figure: Sample CSV Output

3.5.1.3. XML Output

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

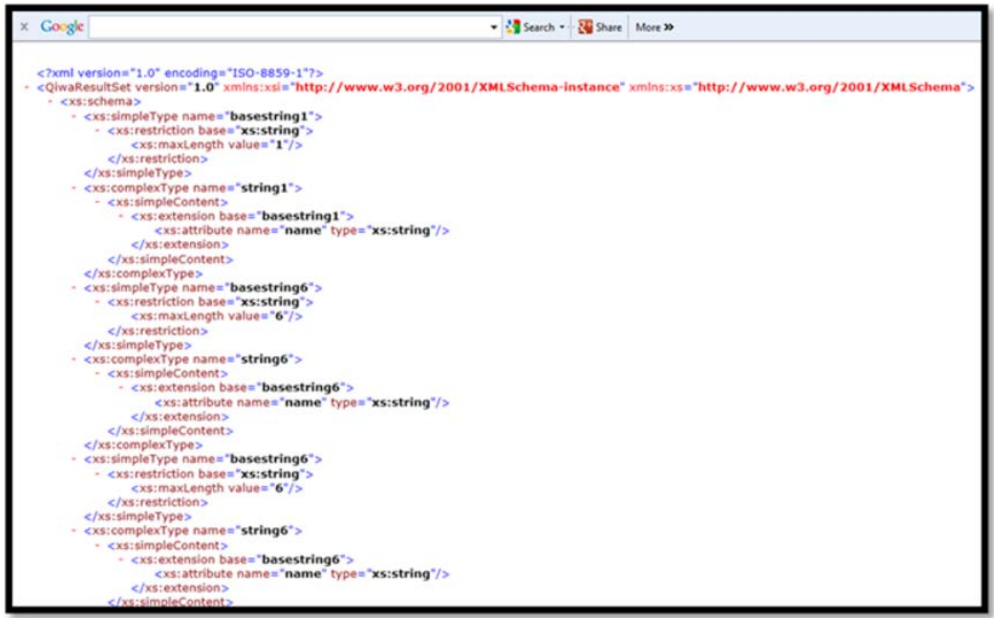


Figure: Sample XML Output

See also: Configure the NetServer

3.5.2. 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.

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	

3.5.3. Resolve Report Failures

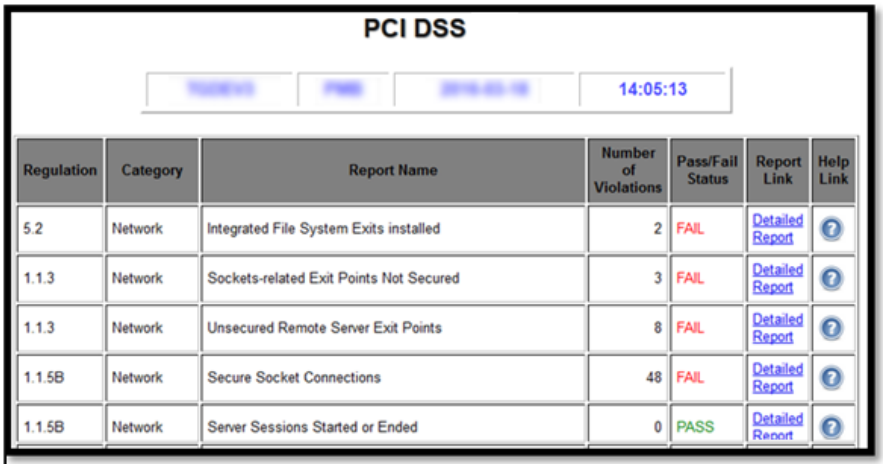
Use this task to resolve report failures. Reports and report cards help you to identify areas within your system that are not properly secured. Once you are aware of these vulnerabilities, the next step is to rectify any issues found.

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	

4. Job Activity Monitor

4.1. Job Activity Monitor

This section describes the basic features of 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

To access the Job Activity Monitor 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 desired monitory activity.
5) Press **Enter**.

4.2. Manage Subsystem

Use this task to manage the subsystem on which you want to monitor batch jobs. This topic describes the following tasks:

- Add subsystems
- Edits subsystem

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

To access the Work with Monitored Subsystems 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 **12** (Work with Monitored Subsystems).

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

4.2.1. 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.
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**.

4.2.2. 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**.

4.3. 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.

4.3.1. 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**.

4.3.2. 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**.

4.4. 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).

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

4.4.1. 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.
3) Identify the user/group to which the rule applies.
4) Enter the following message logging details. These are the details you want 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 used in conjunction with the log level to determine which error messages are sent to job log
Text	Specify the text you want 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**.

4.4.2. 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**.

4.5. 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).

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

4.5.1. 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**.

4.5.2. 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.

4.5.3. Edit User Group

Use this task to edit an exiting 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**.

4.5.4. 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**.

4.6. Display Job Activity

There are several ways to display job activities:

- **Option 1**: View Job Activity Details Via the Job Activity Monitor
- **Option 2**: View Job Activity Summary Report
- **Option 3**: View Job Activity Details Report

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**.

4.6.1. 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.

4.6.1.1. 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**.

Note: The monitored jobs details are displayed in the **Work with Job Activity** screen.

4.6.1.2. 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.

4.6.1.3. 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.

4.6.1.4. Filter Job Details

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

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.

4.6.2. 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.

See also: Working with Report Outputs

4.6.3. 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: Working with Report Outputs

4.7. Archive Job Activity Data

Use this task to archive job activity data. 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.

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.

5. Authority Collection

5.1. Authority Collection

This section describes the basic features of **Authority Collection**. When authority collection is activated, it collects the minimum required authorities and users' current authorities to the objects they access. You can use this information to determine the authorities required for an application to run and help eliminate unnecessary over-authorization.

The product provides you an interface to help make it easier to take advantage of the authority collection feature. It also provides authority collection reporting to allow you to quickly and easily view authority collections for any user.

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

5.2. Manage Authority Collection

Use this task to manage authority collections.

Important: Authority Collections is only available with OS IBM i 7.3. or higher.

You have the following authority management options:

- Start Authority Collection (Main Menu)
- Start Authority Collection (STRAUTCO Command)
- End Authority Collection
- Delete Authority Collection
- Display Collection Details
- Run Authority Collection Report

5.2.1. Start Authority Collection using Main Menu

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

To start authority collection

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection):
3) Press **Enter**.
4) Press the **F6** (Start Collection) function key.
5) 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.

5.2.2. 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.

5.2.3. End Authority Collection

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

To end the authority collection

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection).
3) Press **Enter**.
4) Enter **3** (End Collection) in the **Opt** column associated with the user.
5) Press **Enter**.

Figure: Work with Authority Collection Users

5.2.4. Delete Authority Collection

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

To delete the authority collection

Tip: The authority collection must be ended for the user before deleting the collection.

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

5.2.5. Display Authority Collection

Use this task to display the values on which the authority collection was started for a specified user

To display the authority collection details

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection).
3) Press **Enter**.
4) In the **Opt** column associated with the user, enter **5** (Display Collection Details)
5) Press **Enter**.

5.2.6. Run Authority Collection IFS Report

Use this task to run the Authority Collection report for objects in the Integrated File System (IFS).

To run the Authority Collection IFS report

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **4** (Authority Collection).
3) Press the **F9** (Auth Col IFS Report) function key.
4) Press **Enter**.

Important: For data to show in the report, there must be users enrolled in Authority Collection that have values specified for the following parameters:

- Include DLO
- Include file system objects

Tip: To verify if a user has values specified for these parameters, see **Display Collections Details**.

6. Regulation Report Cards

6.1. Regulation Report Cards

This section provides information about the built-in regulation report cards, which 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.

To access the Regulation Report Cards interface

1) Access the **TGAudit Main** menu.
2) At the **Selection or command** prompt, enter **10** (Regulatory Report Cards).
3) Press **Enter**.

6.2. Payment Card Industry Data Security Standard (PCI DSS)

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.

The following is a sample PCI DSS report in HTML format.

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 Report: Payment Card Industry (PCI) Data Security Standard (DSS)

6.3. Health Insurance Portability and Accountability Act (HIPAA)

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.

Health Insurance Portability and Accountability Act

V174063 2013-10-24 15:09:27

Regulation	Category	Description	Number of Violations	Pass/Fail Status	Report Link
164.304	Network	Remote server exit points not secured	37	FAIL	Detailed Report
164.304	Network	Sockets-related exit points not secured	3	FAIL	Detailed Report
164.304	Resources	Public Authority in Library QGPL Not Exclude	127	FAIL	Detailed Report
164.308	Configuration	Create, change, restore user profiles	0	PASS	Detailed Report
164.308	Network	Intrusion monitor	0	PASS	Detailed Report

Figure: Sample Report: Health Insurance Portability and Accountability Act (HIPAA)

6.4. Federal Information Security Management Act (FISMA)

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

6.5. Sarbanes-Oxley (SOX)

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 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.

6.6. Gramm-Leach-Bliley Act (GLBA)

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 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

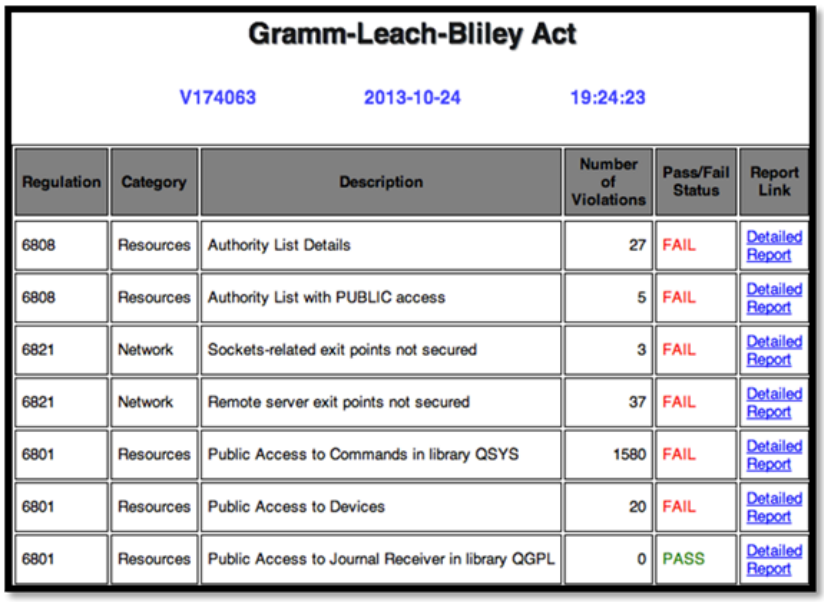
15 USC § 6823 – Criminal penalty

15 USC § 6824 – Relation to State laws

15 USC § 6825 – Agency guidance

15 USC § 6826 – Reports

15 USC § 6827 – Definitions



Gramm-Leach-Bliley Act

V174063 2013-10-24 19:24:23

Regulation	Category	Description	Number of Violations	Pass/Fail Status	Report Link
6808	Resources	Authority List Details	27	FAIL	Detailed Report
6808	Resources	Authority List with PUBLIC access	5	FAIL	Detailed Report
6821	Network	Sockets-related exit points not secured	3	FAIL	Detailed Report
6821	Network	Remote server exit points not secured	37	FAIL	Detailed Report
6801	Resources	Public Access to Commands in library QSYS	1580	FAIL	Detailed Report
6801	Resources	Public Access to Devices	20	FAIL	Detailed Report
6801	Resources	Public Access to Journal Receiver in library QGPL	0	PASS	Detailed Report

Figure: Sample Report: Gramm-Leach-Bliley

6.7. Standards Australia

The Standards 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 latest standard related to information technology — security techniques — guidelines for identification, collection, acquisition, and preservation of digital evidence.

6.8. ISO 27001

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

7. Custom Reports

7.1. Custom Reports

This section describes how to create and manage custom reports.

The reporting engine allows you to customize reports to suit your corporate needs, using a simple report maintenance interface.

Features available through the reporting engine include:

- Defining the columns (collector fields) you want to display in a report
- Defining the selection criteria using operation codes similar to SQL
- Nesting of selection criteria up to 5 levels
- Defining report defaults to optimize report run efficiency

Note: This feature essentially allows you to filter the data source collection from which the report is based so that the report run is as targeted as possible.

- Specially defined date function, which allows you to make date comparisons
- Defining report categories
- Copying existing report definitions

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**.

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

S**ee also:**

Built-in Reports

7.2. Create Reports

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

Step 1 - Add report

Step 1 - Select source from which to collect report data

Step 2 - Name the report

Step 3 - Select the columns you want to include in the report

Step 4 - Define the filter criteria

Step 5 - Define the run-time collector defaults

Step 6 - Confirm the report details

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**.

7.2.1. Add Report

To add a Report

1) Access the **Work with Reports** interface.
2) Press the **F6** (Add Report) function key.
3) Follow the steps in the report wizard.

7.2.2. Select Data Source Collector

Use this task to select the data source collector for your custom report.

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**.

7.2.3. 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 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.

7.2.4. 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.

To select report fields

1) Press the **F4** (Select Fields) function key.
2) Enter **1** in the **Sel** column for each field you want to include as a column in your custom report.
3) Press **Enter**.

Figure: Select Report 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**.

7.2.5. 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.
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.

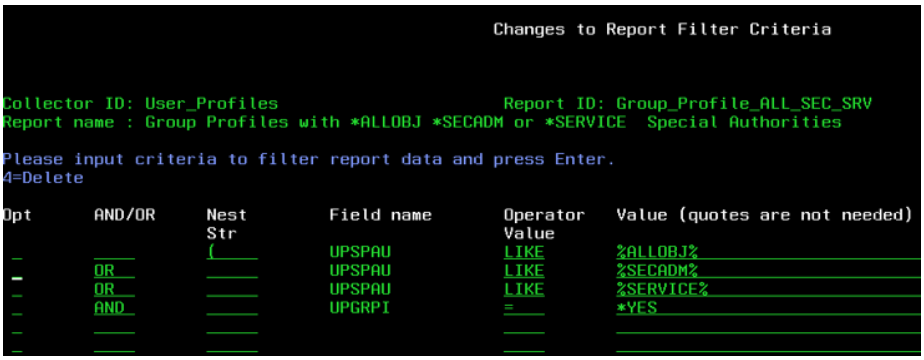


Figure: Build Report Filter Criteria

To delete filter criteria

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

7.2.6. 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.

(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**.

7.2.7. 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**.

7.3. Manage Reports

Use this task to do the following:

- Edit reports
- Copy reports
- Delete reports

To manage 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**.

Note: The **Work with Reports Interface** is displayed.

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

7.3.1. Edit Report

Use this task to edit a report.

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)
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 Lists)	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

7.3.2. 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) Enter **3** in the **Opt** column for the report you want to copy.
3) Enter a unique Report ID and continue customization as desired. Please refer to “Creating Reports” for details.

7.3.3. 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) Access the **Work with Reports** interface.
2) Enter **4** in the **Opt** column for the report you want to delete.

8. Custom Report Cards

8.1. Custom Report Cards

This section describes how to create and manage custom report cards using the **Work with Report Cards** interface (TGWRKCARD). 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.

To access the Work with Report Cards interface

1) Access the **TGAudit 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**.

8.2. Create Report Cards

Use this task to create a customer report card. This task involves multiple steps.
Step 1 - Assign the report card a name
Step 2 - Add reports to the report card
Step 3 - Define the pass criteria for each report
Step 4 - Define the regulation to which the report applies

8.2.1. Define Report Card Name

Use this task to assign the report card a name.

To define the report card name

1) Access the **TGAudit 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.
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.

8.2.2. 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.

Note: 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**.

8.2.3. 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**.

8.2.4. 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**.

8.3. Manage Report Cards

Use this task to do the following

- Edit Report Cards
- Delete Report Cards

8.3.1. 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:

– **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

8.3.2. 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).

9. Product Management

9.1. Product Management

This section describes how to manage the following:

- Product users
- Product licenses
- Product features

Product management is available through the **Product Management** (TGMCONFIG) interface.

To access the Product Management interface

1) Access the **TGAudit Main** menu.
2) Press the **F17** (TG Management) function key.

9.2. Manage User Authorization

Use this task to do the following:

- Add user access
- Delete user access

9.2.1. Add User Access

Use this task to grant a user access to the system.

To add user access

Note: When you grant or remove access you are modifying the authorization list (TGAUTL)

1) Access the **Product Management** interface.
2) At the **Selection or command** prompt, enter **1** (Work with TG Product Users).
3) Press the **F6** (Add new users) function key.
4) Enter the profile name of the user you want to add.
5) Enter ***ALL** in the **Object Authority** column.
6) Press **Enter** twice

9.2.2. Delete User Access

Use this task to revoke user access to the system.

To remove user access

1) Access the **Product Management** interface.
2) At the **Selection or command** prompt, enter **1** (Work with TG Product Users).
3) Delete the text in the **Object Authority** column.
4) Press **Enter**.

9.3. Manage Licensing Status

Use this task to do the following:

- View the license status (expiration date)
- View product version number
- Add a new license key

9.3.1. View License Status

Use this task to view the license status.

To view the status of your license key

1) Access the **Main** menu.
2) Press the **F17** (TG Management) function key.
3) At the **Selection or command** prompt, enter **2** (Licensing Status).
4) Press **Enter**.
5) View expiration date for your license.

Note: The **Work with Licensing Status** interface is displayed.

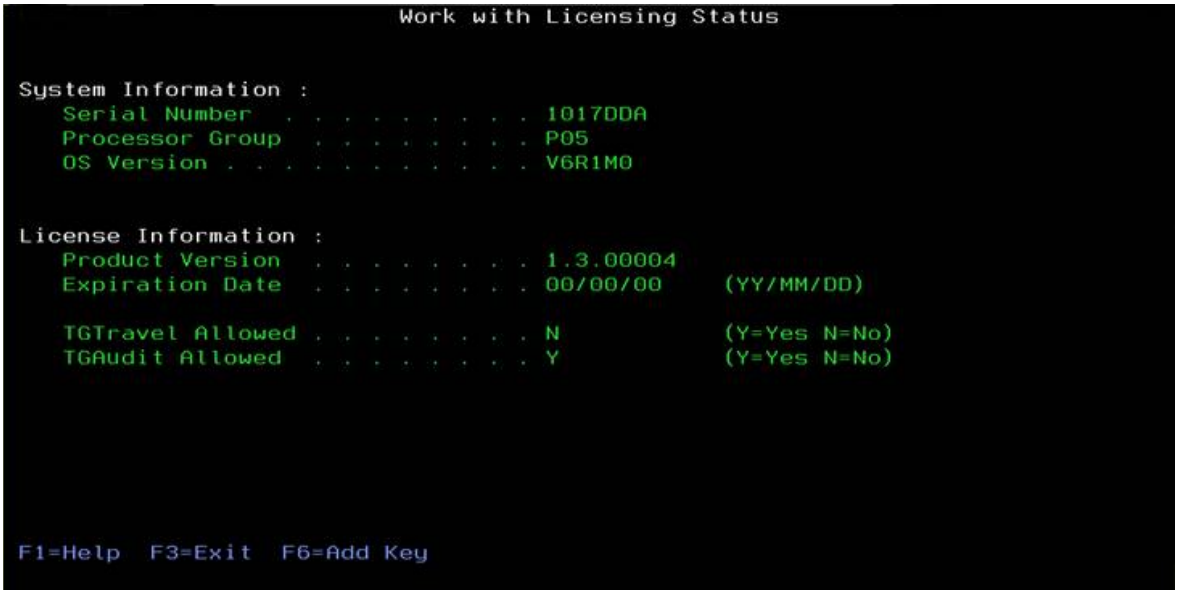


Figure: Work with Licensing Status

9.3.2. View Product Version Number

Use this task to view the product version.

To view the version number

1) Access the **Main** menu.
2) Press the **F17** (TG Management) function key.
3) At the **Selection or command** prompt, enter **2** (Licensing Status).
4) Press **Enter**.

5) View product version.

9.3.3. Add a License Key

Use this task to add a license key.

To add a license key

1) Access the **Work with Licensing Status** interface.
2) Press the **F6** (Add Key) function key.
3) Enter the license key.
4) Press **Enter**.

9.4. Manage Report Outputs

Use this task to edit the configuration file for report outputs.

To edit the report configuration file

1) Access the **Main** menu.
2) Press the **F17** (TG Management) function key.
3) At the **Selection or command** prompt, enter **21** (Report Configuration).
4) Modify the configuration file as necessary.
5) Press the **F3** (Save/Exit) function key.

9.5. Manage HTML Reporting Attributes

Use this task to edit the configuration file for HTML reports.

To edit the HTML configuration file

1) Access the **TGAudit Main** menu.
2) Press the **F17** (TG Management) function key.
3) At the **Selection or command** prompt, enter **22** (HTML Reporting Attributes).
4) Modify the configuration file as necessary.
5) Press **Enter**.

10. Save or Restore Configuration

10.1. Save/Restore TG Configuration

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

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

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

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

See also:

Manager Configuration

10.2. Manager Configuration

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

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

10.2.1. Save Configuration

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

To save the configuration

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

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

4) Complete the following fields:

Field	Description
Product component	Identify the configuration component(s) you want to save. The options available are as follows:

Field	Description
	***ALL** - Save all components ***RPT** - Save reports, report cards settings, and audit configuration ***JAM** - Save JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Save network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Save Access Escalation Manager entitlements **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***SAVE** to create a configuration file--which creates an archive of the current configuration settings-- for the selected product components.

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

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

7) Click **Enter**.

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

10.2.2. Restore Configuration

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

To restore the configuration

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

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

4) Complete the following fields:

Field	Description
Product component	Identify the configuration component(s) you want to restore. Your options are as follows: ***ALL** - Restore all components

Field	Description
	***RPT** - Restore reports, report cards settings, and audit configuration ***JAM** - Restore JAM (Job Activity Monitoring) rules, groups, monitored subsystems, and monitored commands ***NTW** - Restore network socket and exit rules, groups, calendars, exit point configuration, and defaults ***ACC** - Restore AEM (Access Escalation Manager) entitlements, groups, calendars, editors, defaults, and access control **Tip:** If you want to add multiple of components (RPT + JAM), then in the **+ for more values** field, enter a plus sign (+) and then press **Enter**. A column of empty rows appears. Enter each component on a separate row. When you have entered all the desired components, press **Enter** again to return to the **Save/Restore TG Configuration** interface.
Operation to perform	Enter ***RESTORE** to use an existing save file to restore the configuration to a previous state.

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

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

7) Click **Enter**.

10.2.3. Copy Configuration

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

To copy the configuration

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

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

3) Follow the instruction to restore a configuration instance.

See also

Save/Restore TG Configuration

11. Troubleshooting

11.1. FAQ

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

11.1.1. Why does my report has no data?

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

11.2. FAQ

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

11.2.1. Why does my report has no data?

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

11.3. Error Messages

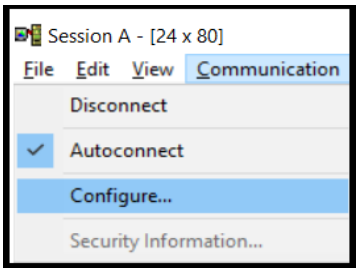
Use this section to learn more about error messages you might encounter.

11.3.1. CPF4169 While Accessing Menu Options

If you encounter a run-time error with message ID CPF4169 while accessing any of the menu options, it is likely that the emulator you are using has a display size of 24x80. The TG interface requires the use of a larger screen size (27x132). To resolve the issue, simply change the emulator session size to 27x132.

To change the emulator display size

1) Access the IBM i **Main** menu.
2) From the session menu, click **Communication | Configure.**



3) In the **Type of emulation** group box, change **Size** to **27x132**.
4) Click **OK**.
5) From the **Session** menu, select **File | Save**. This will update your .ws (Windows JScripit) file.

12. Glossary

12.1. Concepts

This section describes key concepts. These concepts might be existing IBM® i concepts or concepts specific to using TG products. In any case, understanding these concepts should improve your user experience.

The IBM i concepts are described here as they relate to TG products, but if at any time you would like to see the IBM i definitions for these concepts, visit the IBM i documentation portal.

12.2. Activity Monitor Rule

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

12.3. Built-in Reports

A report is a visual representation of data from a collector. The system provides built-in reports, and you can create custom reports as needed.

Note: The built-in reports available are dependent on your license agreement.

12.4. Collectors

A collector is the primary source used to gather data for a report. There are many collectors available for use.

The following is a summary of the general types of data available in collectors:

- User Profile Information
- System Value Data
- System Security Audit Journal (QAUDJRN)
- Database Journal Data
- Data Area Journal Data
- Exit Point Information
- Authority List Data
- Object Authority Information
- Object Details
- Network Status Information

Important: Collectors are required for defining new reports.

See also: For a complete list of available collectors, refer to Appendix A - Collectors.

12.5. Custom Reports

A report is a visual representation of data from a collector. The system provides a set of built-in reports, but you have the ability to create custom reports as needed. Customer reports are unique to each implementation. When defining a custom report, you must configure the following:

- Columns

- Field order
- Selection criteria, which allows you to use SQL-like operators to limit the data returned in the report
- Report defaults, which allow you to customize data the source collection and improve the efficiency of the report

Note: The built-in reports available are dependent on your license agreement.

12.6. Groups

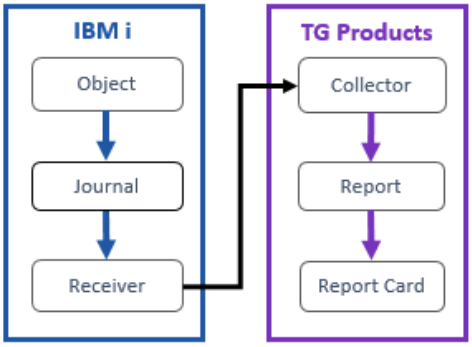
Groups are a means by which to organize system elements (which will be referred to as members). Once you create a group, you can use that group for different purposes. For example, you could use a group as a parameter when defining a rule. Therefore, the rule would apply to all user in the group. You can also use a group as a parameter when generating a report. For example, you might want your report to include information about a network group versus a specific server.

Note: The types of groups and reports available to you are dependent on your license agreement.

12.7. Journals

Journals provide a means by which you can record the activity of an object. This activity is captured in the form of a journal entry and stored in a journal receiver. TG products use collectors to pull data from journal receivers. The data pulled by the collectors is then used to produce reports.

For example, you can use the audit journal (QAUDJRN) to monitor object activity and to log security event.



12.8. Library

A library is a means by which to group related objects and to find objects by name when they are used. Therefore, a library is a directory of grouped objects.

12.9. Receivers

Receives store journal transactions. Transactions are the data elements that document the activities of an object. TG products use collectors to pull transactions from receivers. Those pulled transactions are used to generate reports.

12.10. Report Cards

A report card allows you to group reports together, run them in batch mode, and view the pass/fail status of each individual report included in the report card.

The system provides a set of built-in report cards that group together regulatory compliance reports, and users can create custom report cards as needed.

Regulatory Report Cards

The built-in report cards address the following compliance regulations:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act of 2002 (FISMA)
- Standards Australia
- Information security management system Standard (IS0 27001)

12.11. Rules

A rule allows you to control or limit an action or activity.
Note: The types of rules available to you are dependent on your license agreement.

12.12. User

A user when referenced in this documentation is referring to an individual who required access to the system.

13. APPENDIX - Collectors

Collector Category	Collector Name	Collector ID
Configuration	Job Description Data	Job_Descriptions
Configuration	Message Queue Information	Message_Queue
Configuration	Output Queue Information	Output_Queue
Configuration	Subsystem Autostart Jobs	Subsystem_Autostart
Configuration	Subsystem Communication Entries	Subsystem_Communications
Configuration	Subsystem Information Details	Subsystem_Information
Configuration	Subsystem Job Queue	Subsystem_Job_Queue
Configuration	Subsystem Pool Data	Subsystem_Pool_Data
Configuration	Subsystem Prestart Jobs	Subsystem_Prestart
Configuration	Subsystem Remote Entries	Subsystem_Remote
Configuration	Subsystem Routing Entries	Subsystem_Routing
Configuration	Subsystem Workstation Names	Subsystem_Workstation_Names
Configuration	Subsystem Workstation Types	Subsystem_Workstation_Types
DataAudit	Audit data area changes	Data_Area_Auditing
DataAudit	Monitor Database changes	Database_Auditing
IFS	Display Extended Journaling information for the IFS object	IFS_Journaling
IFS	Display status information about an IFS file	IFS_Status
IFS	Display the Attributes for the IFS objects	IFS_Attributes
IFS	Display the public and private authorities associated with the object	IFS_Authorities
Journal	Access Control List Changes	Journal_VA
Journal	Actions on Validation Lists	Journal_VO
Journal	Actions to IP Rules	Journal_IR
Journal	APPN Endpoint Filter Violations	Journal_NE
Journal	Asynchronous Signals Processed	Journal_SG
Journal	Authority Changes to Restored Objects	Journal_RA
Journal	Authority Collection Data	Authority_Collection

Collector Category	Collector Name	Collector ID
Journal	Authority Failures	Journal_AF
Journal	Authority Restored for User Profiles	Journal_RU
Journal	Authorization List or Object Authority Changes	Journal_CA
Journal	Change Request Descriptor Changes	Journal_CQ
Journal	Change Request Descriptors Restored	Journal_RQ
Journal	Changes to Service Tools Profiles	Journal_DS
Journal	Close Operations on Server Files	Journal_VF
Journal	Cluster Operation	Journal_CU
Journal	Commands Executed	Journal_CD
Journal	Connection Verification	Journal_CV
Journal	Connections Started, Ended, or Rejected	Journal_VC
Journal	Create Operations	Journal_CO
Journal	Cryptographic Configuration Changes	Journal_CY
Journal	Delete Operations	Journal_DO
Journal	Directory Link, Unlink, and Search Operations	Journal_LD
Journal	Directory Search Violations	Journal_ND
Journal	Directory Server Extensions	Journal_XD
Journal	DLO Object Changes	Journal_YC
Journal	DLO Object Reads	Journal_YR
Journal	Dual Optical Object Accesses	Journal_O2
Journal	EIM Attribute Changes	Journal_AU
Journal	Environment Variable Changes	Journal_EV
Journal	Exceeded Account Limit Events	Journal_VL
Journal	Exit Point Maintenance Operations	Journal_GR
Journal	Identity Token Events	Journal_X1
Journal	Internet Security Management Events	Journal_IS
Journal	Inter-process Communication Events	Journal_IP
Journal	Intrusion Monitor Events	Journal_IM
Journal	Invalid Sign-on Attempts	Journal_PW
Journal	Job Changes	Journal_JS
Journal	Job Descriptions – USER Parameter Changes	Journal_JD

Collector Category	Collector Name	Collector ID
Journal	Job Descriptions that Contain User Profile Names were Restored	Journal_RJ
Journal	Key Ring File Changes	Journal_KF
Journal	LDAP Operations	Journal_DI
Journal	Network Attribute Changes	Journal_NA
Journal	Network Authentication Events	Journal_X0
Journal	Network Log On and Off Events	Journal_VN
Journal	Network Password Errors	Journal_VP
Journal	Network Profile Changes	Journal_VU
Journal	Network Resource Accesses	Journal_VR
Journal	Object Auditing Attribute Changes	Journal_AD
Journal	Object Changes	Journal_ZC
Journal	Object Management Changes	Journal_OM
Journal	Object Ownership Changes	Journal_OW
Journal	Object Reads	Journal_ZR
Journal	Objects Restored	Journal_OR
Journal	OfficeVision Mail Services Actions	Journal_ML
Journal	Optical Volume Accesses	Journal_O3
Journal	Ownership Changes for Restored Objects	Journal_RO
Journal	Primary Group Changes	Journal_PG
Journal	Primary Group Changes for Restored Objects	Journal_RZ
Journal	Printer Output Changes	Journal_PO
Journal	Program Changes to Adopt Owner Authority	Journal_PA
Journal	Programs Restored that Adopt Owner Authority	Journal_RP
Journal	Programs that Adopt Authority were Executed	Journal_AP
Journal	PTF Object Changes	Journal_PU
Journal	PTF Operations	Journal_PF
Journal	Row and Column Access Control	Journal_AX
Journal	Secure Socket Connections	Journal_SK
Journal	Server Security User Information Actions	Journal_SO
Journal	Server Sessions Started or Ended	Journal_VS

Collector Category	Collector Name	Collector ID
Journal	Service Status Change Events	Journal_VV
Journal	Service Tools Actions	Journal_ST
Journal	Single Optical Object Accesses	Journal_O1
Journal	Socket Descriptor Details	Journal_GS
Journal	Spooled File Actions	Journal_SF
Journal	Subsystem Routing Entry Changes	Journal_SE
Journal	Swap Profile Events	Journal_PS
Journal	System Directory Changes	Journal_SD
Journal	System Values Changes	Journal_SV
Journal	Systems Management Changes	Journal_SM
Journal	User Profile Changes	Journal_CP
Log	Job Log Details	Job_Log_Details
Log	Job Log Summary	Job_Log_Summary
Network	Controller Attached Device Information	Controller_Attached_Devices
Network	Controller Description Information	Controller_Description_Data
Network	Device Description APPC Information	Device_Description_APPC
Network	Device Description Information	Device_Description_Data
Network	Line Description Information	Line_Description_Data
Network	Network Attribute Information	Network_Attributes
Network	Network Connections Ipv4 and Ipv6	Network_Connections
Network	Network Interface Data Ipv4	Network_Interface_Ipv4
Network	Network Interface Data Ipv6	Network_Interface_Ipv6
Network	Network Route Data Ipv4	Network_Route_Ipv4
Network	Network Route Data Ipv6	Network_Route_Ipv6
Network	Network Server Description Data	Network_Server_Descriptions
Network	Network Server Encryption Status	Network_Svr_Encrypt_Status
Network	TCP/IP Ipv4 Stack Attributes	Network_TCPIP_Ipv4
Network	TCP/IP Ipv6 Stack Attributes	Network_TCPIP_Ipv6
Object	Authorized Users through Authorization Lists	Auth_Users_via_Auth_Lists
Object	Display Field Level Authorities	Field_Authority
Object	Display Object Authority	Object_Authority

Collector Category	Collector Name	Collector ID
Object	Display Object Details	Object_Details
Object	Message Queue Data Details	Message_Queue_Data
Object	Program Reference Data	Program_Reference_Data
System	Authority List Data	Authority_List
System	Basic Information about a software product	Product_Info
System	Display Exit Point Data	Exit_Points
System	Display System Value Data	System_Values
System	Installed Software Resources Data	Software_Resources
System	Program Temporary Fix Data	PTF_Data
System	Service Tool User Data	Service_Tool_Users
Users	Display User Profile Data	User_Profiles
Users	Programs that Adopt Authority	Program_Adopt
Users	User Profile Object Authorities	User_Object_Authorities