NetIQ Security Solutions for IBM i
TGAudit 1.4
User Guide
June 2016

Legal Notice

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

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

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

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

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

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

Copyright © 2013-2016 Trinity Guard LLC. All rights reserved.

Table of Contents

TABLE OF CONTENTS ..... **III**

1. INTRODUCTION **1**

1.1. PRODUCT OVERVIEW 1
1.2. KEY FEATURES 2
1.3. BENEFITS 3

2. INSTALLATION **4**

2.1. IBM I OS REQUIREMENTS 4
2.2. INSTALLATION STEPS 4
2.3. LIBRARIES AND COMMANDS 5

3. CONFIGURATION **6**

3.1. PRODUCT ACCESS 6
3.2. LICENSE KEYS 7
3.3. AUTHORIZING USERS 8
3.4. CONFIGURE NETSERVER TO ENABLE REPORT VIEWING 9
3.5. SET UP SYSTEM AUDITING 16
3.5.1. Security Auditing Journal Details *17*
3.5.2. Change Security Auditing *18*
3.5.3. Set Up Object Auditing *19*
3.5.4. Set Up Integrated File System Auditing *20*
3.5.5. Set Up Database Journaling *20*
3.5.6. Set Up Data Area Journaling *21*
3.5.7. Set Up Range of Journal Receivers for Reports *22*
3.5.8. Journal Receiver Cleanup *23*
3.5.9. Report Data Cleanup *24*

4. REPORTING CONCEPTS **25**

4.1. COLLECTORS 25
4.2. REPORTS 25
4.3. REPORT CARDS 26

5. USING TGAUDIT **27**

5.1. RUNNING REPORTS 27
5.1.1. TGAudit Menu Options *27*
5.1.2. Work with Reports Interface *28*
5.1.3. TGRPT Command Interface *29*
5.2. RUNNING REPORT CARDS 33
5.2.1. TGAudit Menu Options *33*
5.2.2. Work with Report Cards Interface *34*
5.2.3. TGCARD Command Interface *35*
5.3. MANAGING REPORT AND REPORT CARD HISTORY 36
5.4. REPORT OUTPUT TYPES 36
5.4.1. Preview of CSV format *37*
5.4.2. Preview of XML format *37*
5.4.3. Preview of HTML format *38*
5.4.4. Detail views *38*
5.4.5. Report Help *39*

5.5. WHAT DO I DO NEXT? 39

6. JOB ACTIVITY MONITOR 40

6.1. CONFIGURE JOB ACTIVITY MONITORING 41
6.1.1. Configure Batch Jobs 41
6.1.2. Configure Interactive Jobs 42
6.1.3. Configure Activity Monitor Rules 43
6.1.3.1. Working with User Groups to Simplify Activity Monitor Rules 44
6.1.4. Viewing Job Activity 48
6.1.4.1. Option 1. Work with Job Activity 48
6.1.4.2. Option 2. Job Activity Summary Report 49
6.1.4.3. Option 3. Job Activity Details Report 51
6.1.5. Archiving Job Activity Data 52

7. AUTHORITY COLLECTION 54

8. REGULATION REPORT CARDS 58

8.1. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) 59
8.2. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) 60
8.3. FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 62
8.4. SARBANES-OXLEY (SOX) 62
8.5. GRAMM-LEACH-BLILEY ACT (GLBA) 63
Financial Privacy and Safeguards Rule 63
Pretexting protection 63
8.6. STANDARDS AUSTRALIA 64
8.7. ISO 27001 64

9. REPORT CUSTOMIZATION 66

9.1. CREATING REPORTS 66
Step 1 - Define Report Name and Collector 67
Step 2 - Select Report Columns 68
Step 3 - Define Filter Details 71
Step 4 - Define Report Defaults 73
9.2. MODIFYING REPORTS 75
9.3. COPYING REPORTS 75
9.4. DELETING REPORTS 75

10. REPORT CARD CUSTOMIZATION 76

10.1. CREATING REPORT CARDS 76
Step 1 - Define Report Card Name 77
Step 2 - Define Report List 78
Step 3 - Define Pass Criteria 80
Step 4 – Define Regulation Clauses 80
10.2. MODIFYING REPORT CARDS 81
10.3. DELETING REPORT CARDS 81

11. PRODUCT MANAGEMENT 82

Option 1 – Work with TG Product Users 82
Option 2 – Licensing Status 83
Option 21 – Reporting Configuration 83
Option 22 – HTML Reporting Attributes 84

12. TROUBLESHOOTING REFERENCE 85

12.1. UNINSTALL STEPS 85
12.2. CPF4169 WHILE ACCESSING MENU OPTIONS 85
APPENDIX A 86

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 within 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 continuously maintain an optimal level of security on any IBM i or iSeries server.

1.2. Key Features

- Over 220 reports providing built-in security auditing content
- Report Cards allow you to group reports together and view high-level pass/fail results
- Predefined Report Cards map IBM i security auditing data to several major compliance regulations such as PCI, HIPAA, and SOX
- 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 such as HTML, CSV, and XML
- Data sorting in HTML output
- Interface and reporting for IBM i 7.3 Authority Collection security feature
- OS currency

Sample Report Card:

PCI DSS 3.1

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	
2.2.C	Resources	System Security Audit Journal Exists	0	PASS	Detailed Report	
5.1	Resources	Integrated File System Security	1	FAIL	Detailed Report	
2.2.C	Configuration	System, User, and Object Auditing Control Configuration	0	PASS	Detailed Report	
10.2	Configuration	Attention Events are Audited	0	PASS	Detailed Report	
10.2	Configuration	Authorization Failures are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Object Creations are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Deletions of External Objects on the System are Audited	0	PASS	Detailed Report	
10.2	Configuration	Actions that Affect a Job are Audited	0	PASS	Detailed Report	
10.2	Configuration	Networking and Communications Functions are Audited	0	PASS	Detailed	

Sample Report:

Secure Socket Connections For User: *ALL From: 2016-03-18 00:00:00 To: 2016-03-18 14:04:48

Sequence number	Timestamp	Job name	User name	Job number	Program name	Program library	User profile	System name	Remote port	Remote address	Entry type	Local IP address	Local port	Remote IP address	Remote port	Socket descriptor	Filter description	Filter data	Filter data	Address Family
00000000000000148693	2016-03-18-01.35.36.661616	QZSOSMAPD	QUSER	3129	QZSOSMAPD	QSYS	QUSER	TGDEV3	63536	10.11.12.45	A		449		63536	2		0		*IPV6
00000000000000148694	2016-03-18-01.35.37.296336	QZSCSRVSD	QUSER	3123	QZSCSRVSD	QSYS	QUSER	TGDEV3	63537	10.11.12.45	A		8470		63537	2		0		*IPV6
00000000000000150187	2016-03-18-04.15.54.015920	QZSOSMAPD	QUSER	3129	QZSOSMAPD	QSYS	QUSER	TGDEV3	49353	10.11.12.41	A		449		49353	2		0		*IPV6
00000000000000150188	2016-03-18-04.15.54.659504	QZSOSGND	QUSER	3127	QZSOSGND	QSYS	QUSER	TGDEV3	49354	10.11.12.41	A		8476		49354	2		0		*IPV6
00000000000000150196	2016-03-18-04.15.58.127920	QZSOSMAPD	QUSER	3129	QZSOSMAPD	QSYS	QUSER	TGDEV3	49358	10.11.12.41	A		449		49358	2		0		*IPV6
00000000000000150197	2016-03-18-04.15.58.795920	QZSCSRVSD	QUSER	3123	QZSCSRVSD	QSYS	QUSER	TGDEV3	49359	10.11.12.41	A		8470		49359	2		0		*IPV6
00000000000000150337	2016-03-18-04.28.47.800048	QTFTP00015	QTCP	2994	QTMFSRVR	QTCP	QTCP	TGDEV3	49371	10.11.12.41	A		21		49371	2		0		*IPV6
00000000000000150376	2016-03-18-04.30.55.643504	QTFTP00015	QTCP	2994	QTMFSRVR	QTCP	KAPILA	TGDEV3	49371	10.11.12.41	C		20		49373	0		0		*IPV6
00000000000000151056	2016-03-18-05.45.03.280992	QZSOSMAPD	QUSER	3129	QZSOSMAPD	QSYS	QUSER	TGDEV3	49852	10.11.12.41	A		449		49852	2		0		*IPV6
00000000000000151057	2016-03-18-05.45.03.931984	QZSCSRVSD	QUSER	3123	QZSCSRVSD	QSYS	QUSER	TGDEV3	49853	10.11.12.41	A		8470		49853	2		0		*IPV6
00000000000000151284	2016-03-18-06.08.52.980864	QZSOSMAPD	QUSER	3129	QZSOSMAPD	QSYS	QUSER	TGDEV3	49973	10.11.12.33	A		449		49973	2		0		*IPV6
00000000000000151285	2016-03-18-06.08.53.639729	QZSCSRVSD	QUSER	3123	QZSCSRVSD	QSYS	QUSER	TGDEV3	49974	10.11.12.33	A		8470		49974	2		0		*IPV6

1.3. 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

2. Installation

2.1. IBM i OS Requirements

This product is supported on the following OS versions:

- V5R4
- V6R1
- V7R1
- V7R2
- V7R3

TGAudit should be used with 27x132 emulation display. The product is not supported in 24x80 workstation displays.

2.2. Installation Steps

1) Unzip TGINSTALL.zip to desired location on PC
2) Transfer tginstall.svf save file to IBM i system:
   a) At a Windows Command Prompt, type the following to log in to the FTP server on the IBM i and press ENTER:

      FTP *<IBM i system name>*

      Authenticate to IBM i server when prompted.

   b) At the FTP prompt, execute the following commands:

      i) Change transfer mode to binary:

         BIN

      ii) Create save file on IBM i server:

         QUOTE RCMD CRTSAVF QGPL/TGINSTALL

      iii) Transfer tginstall.svf to IBM i server:

         PUT c:*<path to>tginstall.svf* QGPL/TGINSTALL**

      iv) Restore TGINSTALL library:

         QUOTE RCMD RSTLIB TGINSTALL DEV(*SAVF) SAVF(QGPL/TGINSTALL) MBROPT(*ALL) ALWOBJDIF(*ALL)

      v) Run installer:

         QUOTE RCMD TGINSTALL/TGINSTALL PROD(*TGAUDIT) INSTYPE(*INSTALL) EULA(*ACCEPT) BATCH(*NO)

3) Configure TGAudit for use by following the instructions in Chapter 3. Configuration.

2.3. Libraries and Commands

TGAudit installs the following libraries:

- TGPROD
- TGDATA
- TGINSTALL

The following are helpful commands installed in the QGPL library for quick access to TGAudit functions:

- TGMENU – TGAudit Main Menu
- TGRPT – Run a Report
- TGCARD – Run Report Card
- TGWRKRPT – Work with Reports
- TGWRKCARD – Work with Report Cards
- TGLICSTS – Work with Licensing Status

3. Configuration

3.1. Product Access

Sign on to the IBM i using a user profile with *SECOFR user class. At an IBM i command line, type **TGMENU** and press Enter.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

    80. Product Management
                                                                        Bottom
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
Copyright © 2013-2016 Trinity Guard LLC. All rights reserved.
```

3.2. License Keys

A valid license key is required to use TGAudit. A 14-day trial license is provided at the time TGAudit is installed.

If a valid license key is not present, a message will appear in the System Operator (QSYSOPR) message queue.

For help obtaining new license keys, you can contact support@netiq.com.

To enable the product with a new license key, use the “F6=Add Key” function key to type in the new key and press Enter.

Current licensing status can be verified through the “Work with Licensing Status” screen by using the following options: TGMENU -> F17=TG Management -> 2. Licensing Status

```
                         Work with Licensing Status


System Information :
   Serial Number  . . . . . . . . . . 1017DDA
   Processor Group  . . . . . . . . . P05
   OS Version . . . . . . . . . . . . V6R1M0


License Information :
   Product Version  . . . . . . . . . 1.3.00004
   Expiration Date  . . . . . . . . . 00/00/00     (YY/MM/DD)

   TGTravel Allowed . . . . . . . . . N            (Y=Yes N=No)
   TGAudit Allowed  . . . . . . . . . Y            (Y=Yes N=No)





F1=Help  F3=Exit  F6=Add Key
```

3.3. Authorizing Users

During installation, the following users are automatically authorized to use TGAudit:

- QSECOFR
- The user profile that installed the product

To display TGAudit authorized users, use the following options:

- TGMENU -> F17=TG Management -> 1. Work with TG Product Users

Additional users may be authorized to the product by accessing the “Work with TG Product Users” screen by using the following options: TGMENU -> F17=TG Management -> 1. Work with TG Product Users -> F6=Add new users

1. In the 'User' column, enter the name of the user profile you want to authorize
2. In the 'Object Authority' column, enter *ALL
3. Press Enter twice

```
                              Edit Authorization List

Object . . . . . . . :   TGAUTL          Owner  . . . . . . . :   QSECOFR
  Library  . . . . . :     QSYS          Primary group  . . . :   *NONE

Type changes to current authorities, press Enter.

             Object    List
User        Authority  Mgt
*PUBLIC     *EXCLUDE    _
QSECOFR     *ALL        X
ARP         *ALL        _

                                                                      Bottom
F3=Exit   F5=Refresh   F6=Add new users
F11=Display detail object authorities   F12=Cancel   F24=More keys
```

3.4. Configure NetServer to Enable Report Viewing

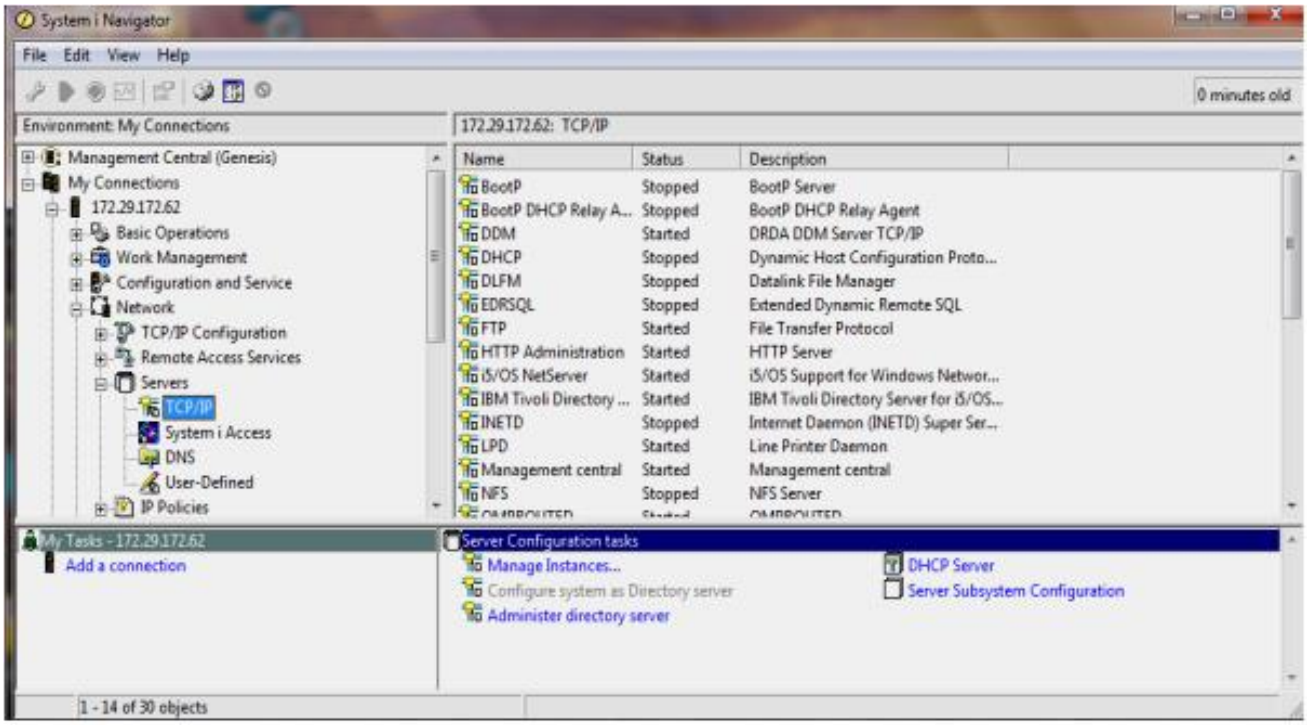
NetServer must be configured in order to take advantage of the automatic display feature for HTML, XML, and CSV report output types. When either of these report output types is selected for an interactive run of a report, the report output will automatically display results on your PC. To take advantage of this feature, follow the steps below to configure a reports folder in i5/OS NetServer.

1) If it is not already started, start NetServer. At an i5/OS command line, type the following and press Enter:

   STRTCPSVR SERVER(*NETSVR)

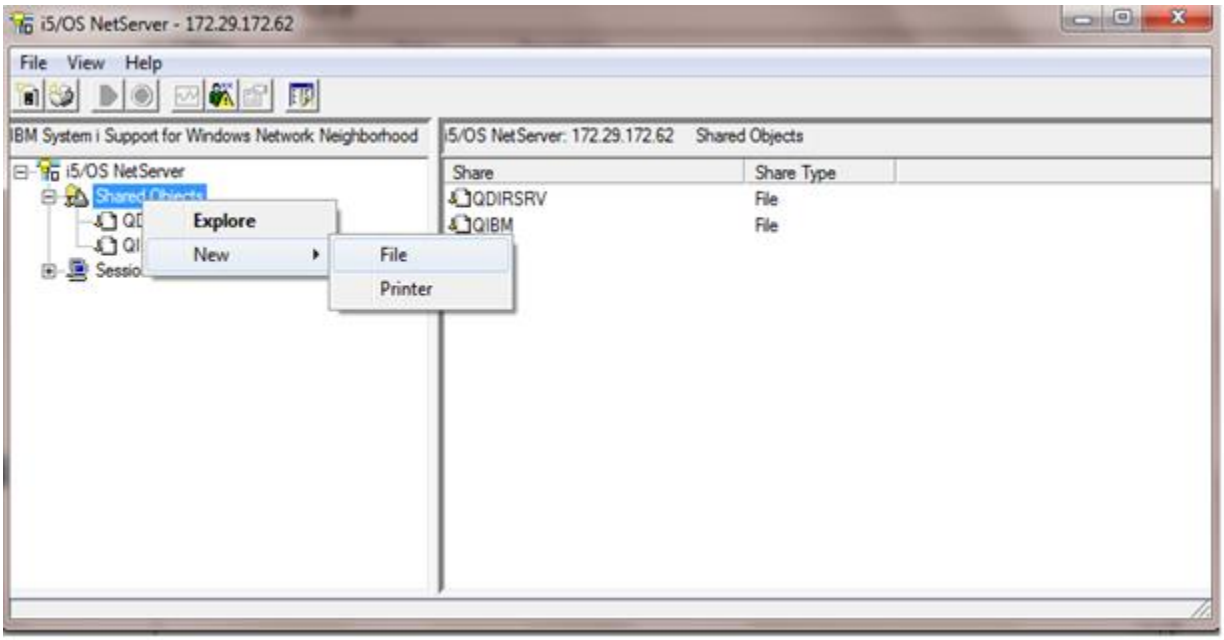
2) Create a NetServer file share called /TrinityGuard:

   a) **System i Navigator → Network → Servers → TCP/IP**

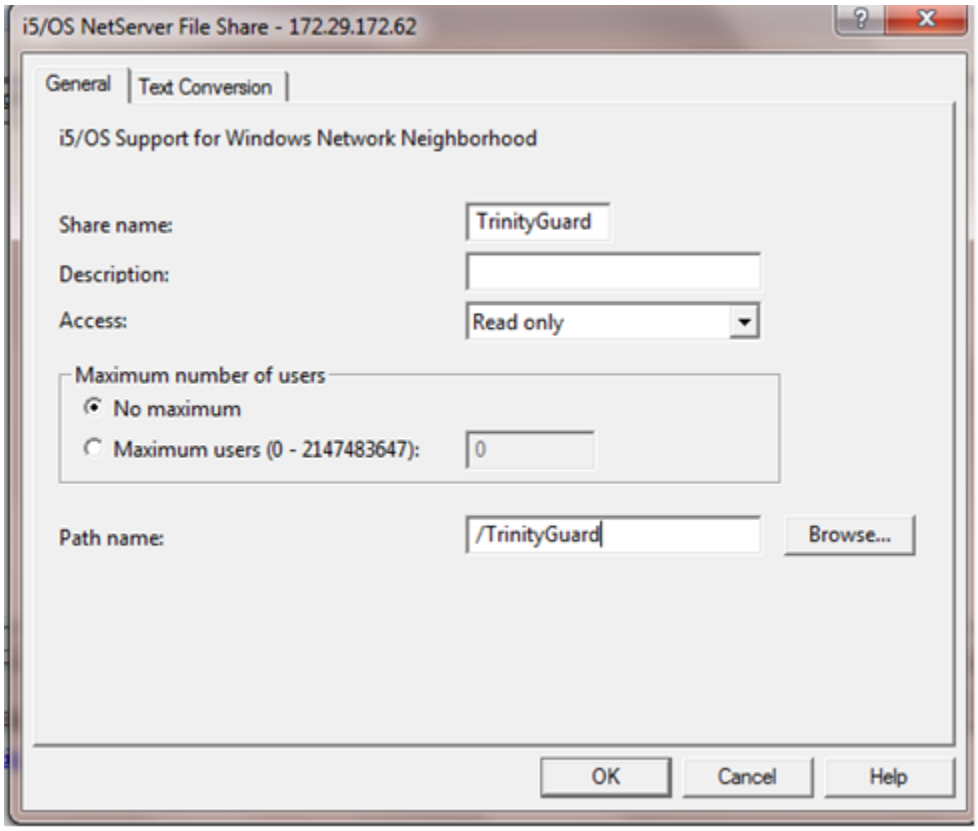


i) Right-click i5/OS NetServer and select Open.

(1) Right-click Shared Objects -> Select New -> Select File

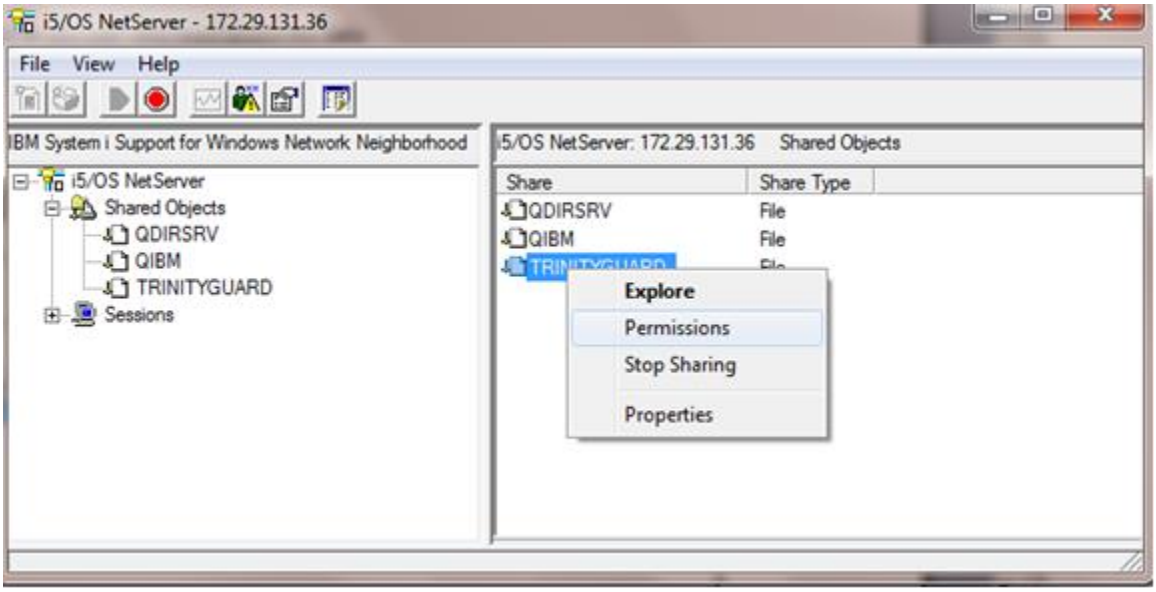


(a) Use the General Properties page to configure the new file share with a name, description, access, maximum number of users, and directory path name, then click OK.

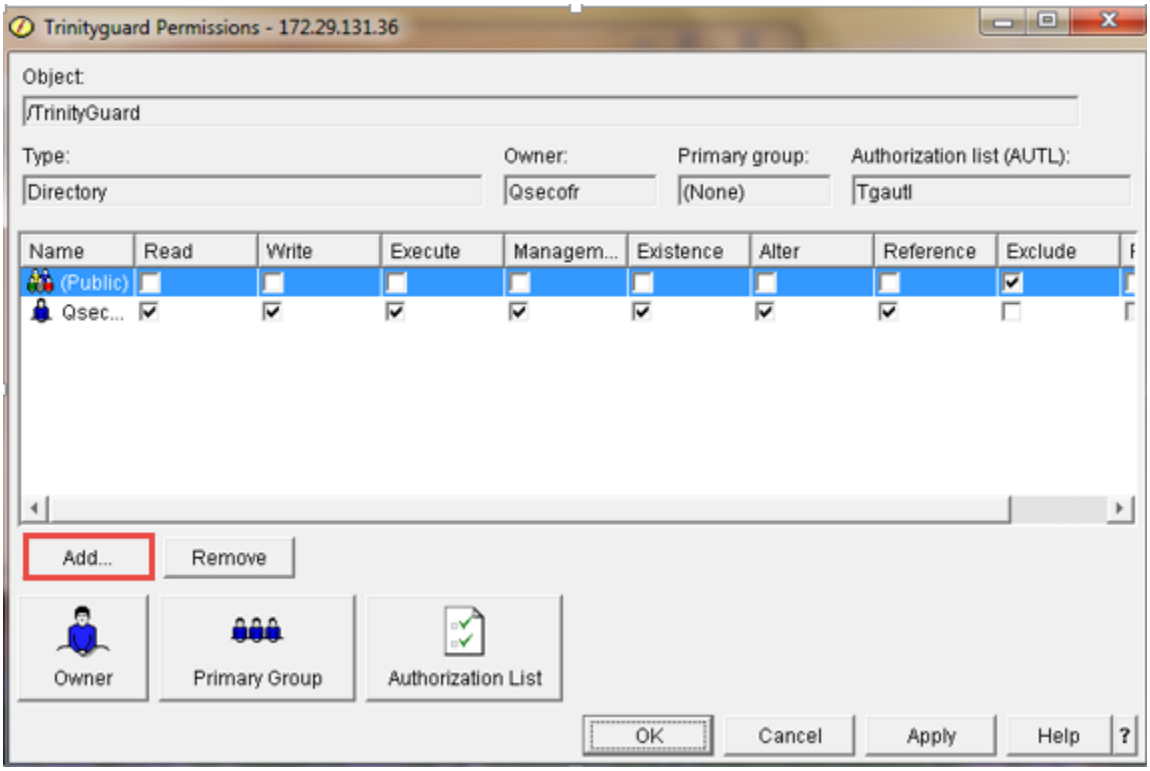


3) Since this IFS folder will contain TGAudit report output with system security-related content, it is important to ensure permissions to this folder are restricted to only those individuals with appropriate job-related responsibilities requiring them to have access. Set permissions to the folder accordingly.

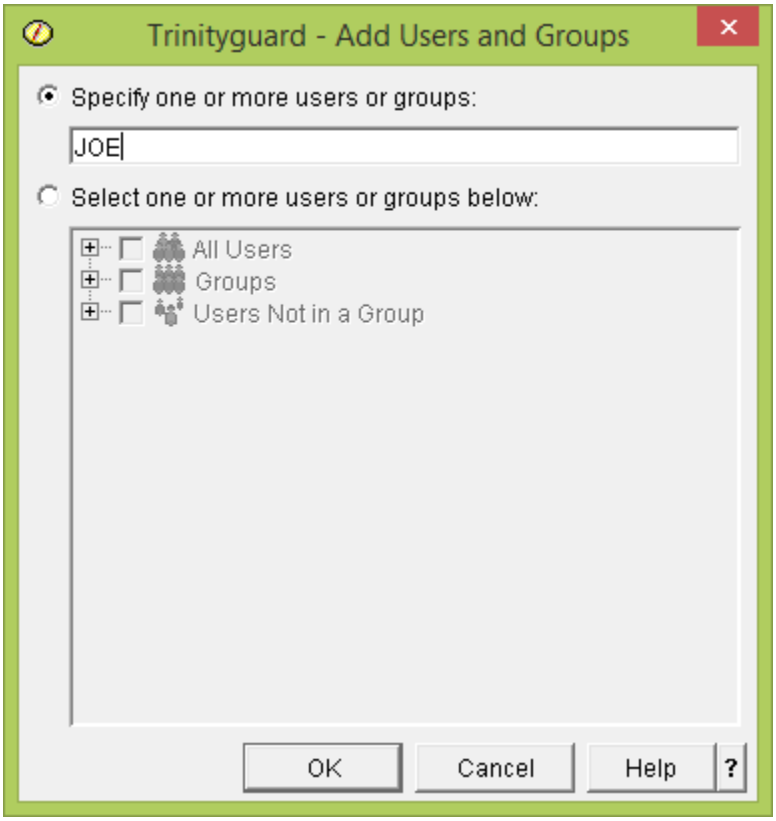
a) To configure individual user access to the share, right click on the TRINITYGUARD share, and select "Permissions."



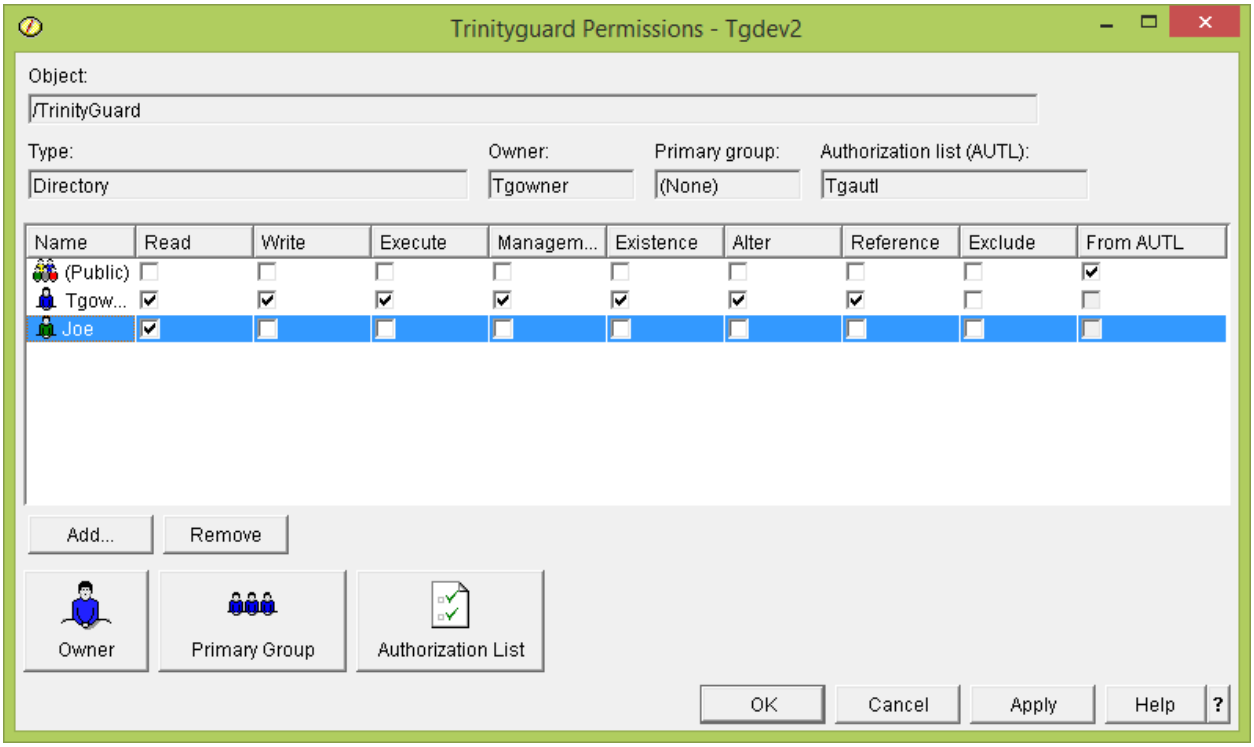
b) Click on the "Add" button:



c) Type the user profile to be granted permission to the new share and click OK.

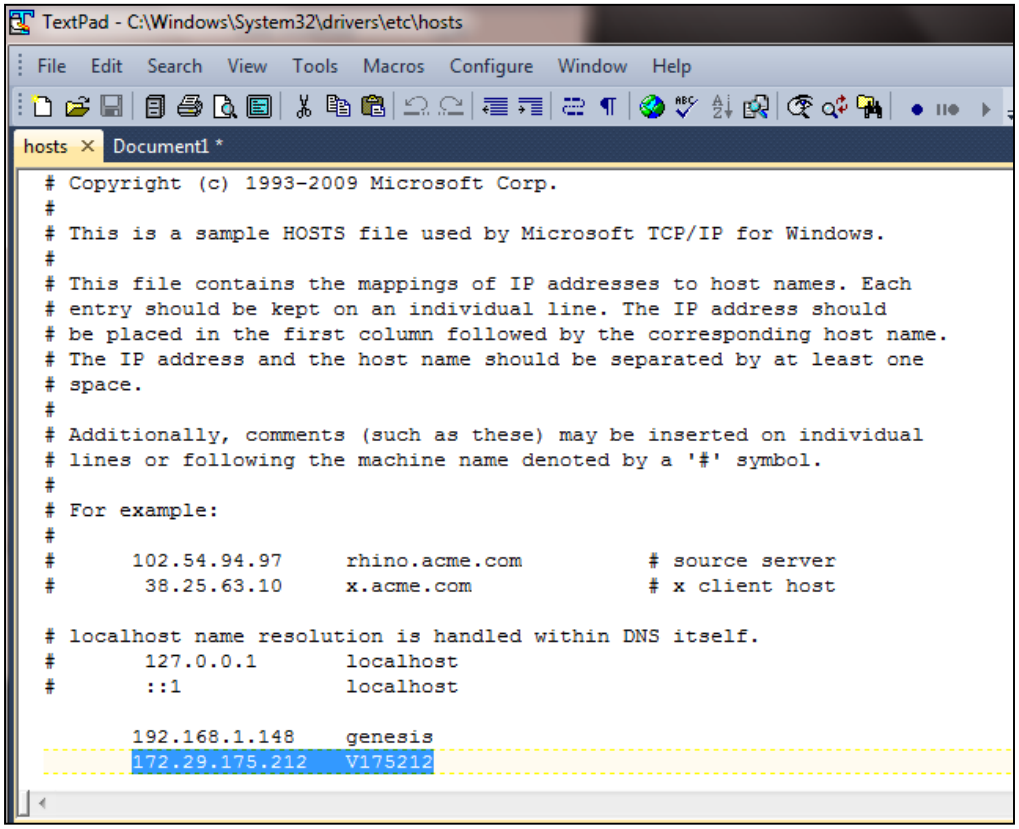


d) Check/uncheck the desired permissions boxes for the user and click OK.



e) Note that, by default, when a user is authorized to TGAudit through the green screen menu, permissions to this folder will be inherited for those users through the product authorization list.

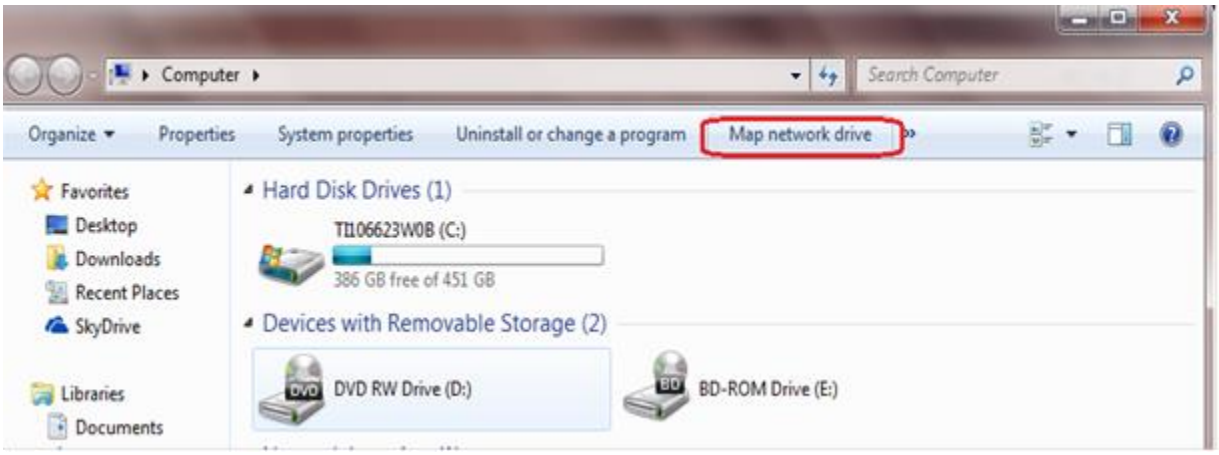
4) Update the hosts table on your PC to include the IBM i server IP address and server name if it does not already exist. To add your IBM i server to the hosts table, use a text editor to edit file C:\Windows\System32\drivers\etc\hosts:



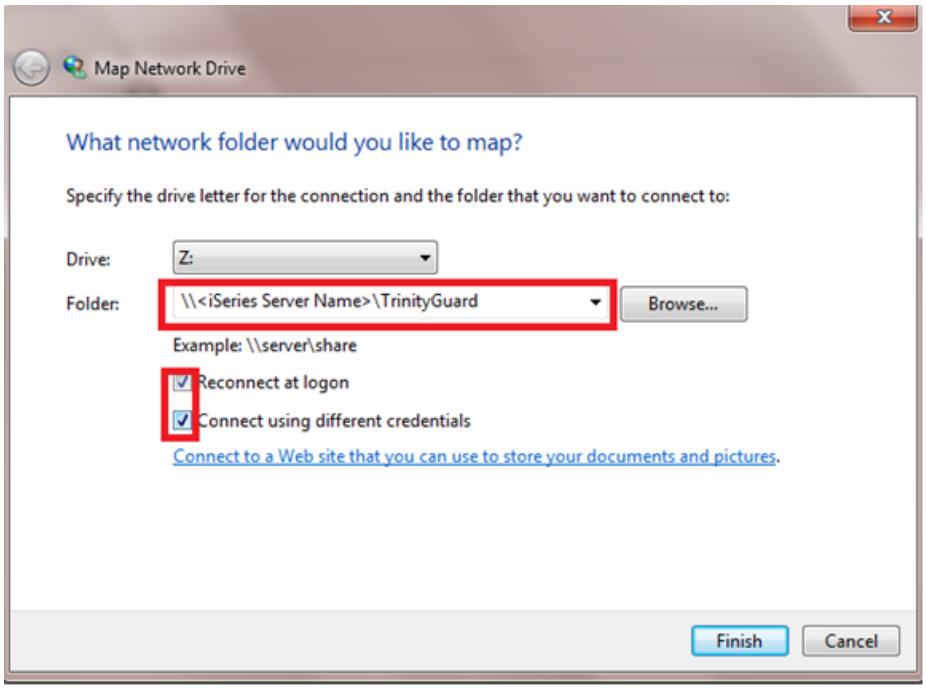
5) Map a network drive on your PC to the newly created folder. (Options may vary slightly depending on your PC OS version.)

   a. Open My Computer

      i) Click on Map Network Drive



(1) Select a drive letter and enter the path to the TrinityGuard folder.
Important: Use the IBM i system name, not the IP address.
Also, ensure both checkboxes are checked for "Reconnect at logon" and "Connect using different credentials."



(2) Click finish and you will be prompted for your user name and password. Enter your i5/OS user profile and password. Click the "Remember my credentials" checkbox and click OK.

b) As an alternate option to map the network drive, from a Windows Command Prompt, enter the following command:

NET USE * *<IBM i Server Name>*\TrinityGuard /USER:IBM i-username IBM i-password

3.5. Set Up System Auditing

In order for many TGAudit reports to contain data, and to ensure you have a clear view into the security state of you system, it is critical that system security auditing is enabled. Using the options in the “Audit Configuration” menu, you gain easy access to system commands that quickly allow you to update your system security audit settings and begin collecting pertinent security audit data.

Note that these options access system commands and the changes made affect the whole system. The changes effective from these menu options are not just local to TGAudit. Therefore, you may need to work with your operations team to make considerations for storage for the security audit journal receivers. The size required for the journal receivers will be based on the unique needs of your environment, the auditing required to meet your security policy, and the amount of usage on the server.

To access the “Audit Configuration” menu, select option 32 from the TGAudit main menu.

```
TGMAUDCFG                        Audit Configuration

Select one of the following:

     1. Security Auditing Journal Details
     2. Change Security Auditing
     3. Set Up Object Auditing
     4. Set Up Integrated File System Auditing
     5. Set Up Database Journaling
     6. Set Up Data Area Journaling
     7. Set Up Range of Journal Receivers for Reports
     8. Journal Receiver Cleanup
     9. Report Data Cleanup

                                                                      Bottom
Selection or command
===> _
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F18=Run Report
F20=Report History
```

3.5.1. Security Auditing Journal Details

Option 1 from the “Audit Configuration” menu displays the system security audit journal (QAUDJRN) details.

If this screen returns the message, “Object QAUDJRN in library *LIBL not found,” it means auditing is not set up, so there is no visibility into security-related activity happening on the system. Without auditing configured, many TGAudit reports are not able to return data.

To automatically create the system security audit journal (QAUDJRN), see option 2 of the “Audit Configuration” menu.

If the system security audit journal exists, a screen similar to the following will be displayed:

```
                          Work with Journal Attributes

 Journal  . . . . . . :   QAUDJRN         Library  . . . . . . :   QSYS

 Attached receiver  . :   AUDRCV0003      Library  . . . . . . :   QGPL

 Text . . . . . . . . :   *BLANK

 ASP  . . . . . . . . :   1               Journaled objects:
 Message queue  . . . :   QSYSOPR           Current  . . . . . :         3
   Library  . . . . . :     *LIBL           Maximum  . . . . . :    250000
 Manage receivers . . :   *SYSTEM         Recovery count . . . :   *SYSDFT
 Delete receivers . . :   *NO             Receiver size options:   *RMVINTENT
 Journal cache  . . . :   *NO                                      *MAXOPT2
 Manage delay . . . . :   10
 Delete delay . . . . :   10
 Journal type . . . . :   *LOCAL
 Journal state  . . . :   *ACTIVE
 Minimize entry data  :   *NONE

                                                                        More...
 F3=Exit   F5=Refresh   F12=Cancel   F17=Display attached receiver attributes
 F19=Display journaled objects       F24=More keys
```

3.5.2. Change Security Auditing

Option 2 from the "Audit Configuration" menu allows you to set up and change audit settings related to the system security audit journal, QAUDJRN. Optionally, the CHGSECAUD command can be used at a command line.

```
                    Change Security Auditing (CHGSECAUD)

 Type choices, press Enter.

 QAUDCTL system value . . . . . .   *AUDLVL      *SAME, *ALL, *NONE...
                                    *OBJAUD
                                    *NOQTEMP
 Auditing values  . . . . . . . .   *AUTFAIL     *SAME, *ALL, *DFTSET...
                                    *CREATE
                                    *DELETE
                                    *OBJMGT
                                    *PGMADP
                                    *PGMFAIL
                                    *PRTDTA
                                    *SAVRST
                                    *SECURITY
                                    *SERVICE
                + for more values   *SYSMGT
 Initial journal receiver . . . .   AUDRCV0001    Name
   Library  . . . . . . . . . . .     QGPL        Name, *CURLIB
                                                                    Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Note that if the security audit journal does not exist when this command is issued, it will be created along with its initial journal receiver. Audit data gathered due to the configuration of this command is stored in the QAUDJRN journal receiver. The values configured in this option should be decided upon based on your security policy requirements.

3.5.3. Set Up Object Auditing

Option 3 from the “Audit Configuration” menu allows you to set up object level auditing for specific sensitive objects on the system that require close monitoring. Optionally, the CHGOBJAUD command can be used at a command line.

```
                        Change Object Auditing (CHGOBJAUD)

 Type choices, press Enter.

 Object . . . . . . . . . . . . . .   __________     Name, generic*, *ALL
   Library  . . . . . . . . . . . .     *LIBL_____   Name, *LIBL, *USRLIBL...
 Object type  . . . . . . . . . . .   _______        *ALL, *ALRTBL, *AUTHLR...
 ASP device . . . . . . . . . . . .   *__________    Name, *, *SYSBAS
 Object auditing value  . . . . .   _______          *NONE, *USRPRF, *CHANGE, *ALL

                                                                            Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Note that for object level auditing to be enabled, system value QAUDCTL must also be set to include value *OBJAUD. The QAUDCTL system value can be set using option 2, “Change Security Auditing,” if desired.

3.5.4. Set Up Integrated File System Auditing

Option 4 from the “Audit Configuration” menu allows you to configure auditing for the Integrated File System (IFS). Optionally, the CHGAUD command can be used at a command line.

```
                         Change Auditing Value (CHGAUD)

 Type choices, press Enter.

 Object . . . . . . . . . . . . . .   _
_____
 Object auditing value  . . . . .   *NONE__        *NONE, *USRPRF, *CHANGE, *ALL
 Directory subtree  . . . . . . .   *NONE          *NONE, *ALL
 Symbolic link  . . . . . . . . .   *NO_           *NO, *YES

                                                                            Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

3.5.5. Set Up Database Journaling

Option 5 from the “Audit Configuration” menu allows you to start auditing DB2 database files on the system. Optionally, the STRJRNPF command can be used at a command line.

```
                     Start Journal Physical File (STRJRNPF)

 Type choices, press Enter.

 Physical file to be journaled  .   __________      Name, generic*, *ALL
   Library  . . . . . . . . . . .     *LIBL_____    Name, *LIBL, *CURLIB
                + for more values   __________
                                      *LIBL_____
 Journal  . . . . . . . . . . . .   __________      Name
   Library  . . . . . . . . . . .     *LIBL_____    Name, *LIBL, *CURLIB
 Record images  . . . . . . . . . > *BOTH          *AFTER, *BOTH
 Journal entries to be omitted  .   *NONE__        *NONE, *OPNCLO
 Logging level  . . . . . . . . .   *ERRORS        *ERRORS, *ALL

                                                                            Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

After journaling is started for a physical file, you can produce reports through TGAudit to see the detailed changes happening to that file, down to the field-level. Before and after images of changes to the file are captured and

enable you to trace changes quickly and efficiently with “Database Change” reports available in the “Data Level Reports” menu.

3.5.6. Set Up Data Area Journaling

Option 6 from the “Audit Configuration” menu enables you to start auditing for data areas. Optionally, the STRJRNOBJ command can be used at a command line.

```
                        Start Journal Object (STRJRNOBJ)

 Type choices, press Enter.

 Object . . . . . . . . . . . . . .   __________     Name, generic*, *ALL
   Library  . . . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB
                + for more values    __________
                                       *LIBL
 Object type  . . . . . . . . . . . > *DTAARA        *DTAARA, *DTAQ
 Journal  . . . . . . . . . . . . .   __________     Name
   Library  . . . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB
 Images . . . . . . . . . . . . . . > *BOTH         *AFTER, *BOTH
 Logging level  . . . . . . . . . .   *ERRORS       *ERRORS, *ALL

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

After journaling is started for a data area, you can produce reports through TGAudit to see the detailed changes happening to that data area. Before and after images of changes to the data area are captured and enable you to trace changes quickly and efficiently with “Data Area Changes” reports available in the “Data Level Reports” menu.

3.5.7. Set Up Range of Journal Receivers for Reports

Option 7 from the “Audit Configuration” menu allows you to configure the journal receiver range TGAudit will use for running reports.

```
                        TG Journal Attributes (TGJRNATR)

 Type choices, press Enter.

 Range of journal receivers:
   Starting journal receiver  . .   *CURCHAIN    Name, *CURRENT, *CURCHAIN
     Library  . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB
   Ending journal receiver  . . .   __________   Name, *CURRENT
     Library  . . . . . . . . . .     *LIBL      Name, *LIBL, *CURLIB

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

3.5.8. Journal Receiver Cleanup

Option 8 from the "Audit Configuration" menu provides a tool to help you effectively clean up journal receivers for any journal. Journal receivers tend to consume a lot of disk space and, depending on your system activity, can grow very fast.

Before using this tool, verify your data retention policy and make sure you save the receivers to media for later retrieval. In case of a security incident investigation, old receiver data is required to do forensic analysis.

```
                         TG Journal Cleanup (TGDURNATOR)

 Type choices, press Enter.

 Journal  . . . . . . . . . . . . .   QAUDJRN    Name
   Library  . . . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
 Journal data retention days? . .   00060        00001-99999
 Delete unsaved data? . . . . . .   *NO          *YES, *NO
 Run interactively? . . . . . . .   *NO          *YES, *NO
 Job queue  . . . . . . . . . . .   QBATCH       Name, *NONE
   Library  . . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
 Schedule?  . . . . . . . . . . .   *NO          *YES, *NO

                                                                    Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Journal
Specify the journal name from which the journal receivers are to be deleted.

Library
Specify the name of the library where the journal resides.

Journal data retention days?
Specify the number of days of journal data to be retained. For example, if you specify 60 days, you will retain all journal receivers containing the last 60 days of journal data.

Delete unsaved data?
*YES – Journal data associated with the journal will be deleted regardless of if it was saved previously.
*NO – Only data previously saved to media will be deleted.

Run interactively?
*YES – Executes the TGDURNATOR command interactively.
*NO – Submits the TGDURNATOR command to run in batch.

Job Queue
Specify the job queue in which the job will run. This parameter is only valid for batch jobs.

Job Queue Library
Specify the library where the job queue resides. This parameter is only valid for batch jobs.

Schedule?
*YES – The job is scheduled using IBM's job scheduler. The default job name given is TGJRNCLEAN. IBM job scheduler options are displayed and can be edited as desired.
*NO – The job is not scheduled.

3.5.9. Report Data Cleanup

Option 9 from the "Audit Configuration" menu allows you to manage HTML report data stored in the IFS. Report data can be automatically purged on a scheduled basis using this option.

```
                        TG Report Data Cleanup (TGRPTCLEAN)

 Type choices, press Enter.

 Report data retention days?  . .   _____          00001-99999
 Archive? . . . . . . . . . . . .   *NO            *YES, *NO
 Archive File . . . . . . . . . .   __________     Name
   Library  . . . . . . . . . . .     QGPL_______  Name, *CURLIB
 Run interactively? . . . . . . .   *NO            *YES, *NO
 Job queue  . . . . . . . . . . .   QBATCH____     Name, *NONE
   Library  . . . . . . . . . . .     *LIBL______  Name, *LIBL, *CURLIB
 Schedule?  . . . . . . . . . . .   *NO            *YES, *NO

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Report data retention days?
Specify the number of days to retain HTML reports stored in the IFS. The reports within this number of days are not deleted when this command is run. The reports older than this number of days are deleted when this command is run.

Archive?
*YES – All TGAudit HTML report data stored on the IFS will be saved to an archive save file.
*NO – HTML report data will not be archived.

Archive File
Specify the name of the save file where HTML reports will be archived.

Library
Specify the library name where the save file to archive HTML reports exists.

Run interactively?
*YES – Executes the TGRPTCLEAN command interactively.
*NO – Submits the TGRPTCLEAN command to run in batch.

Job Queue
Specify the job queue in which the job will run. This parameter is only valid for batch jobs.

Job Queue Library
Specify the library where the job queue resides. This parameter is only valid for batch jobs.

Schedule?
*YES – The job is scheduled using IBM's job scheduler. The default job name given is TGJRNCLEAN. IBM job scheduler options are displayed and can be edited as desired.
*NO – The job is not scheduled.

4. Reporting Concepts

This chapter outlines the overall reporting concepts of TGAudit. For details on how to run reports and Report Cards, please refer to Chapter 5, "Using TGAudit." For details on customizing reports and Report Cards, please refer to Chapters 8 and 9, "Report Customization" and "Report Card Customization."

4.1. Collectors

The primary source used to gather data for a report is called a Collector. There are many Collectors available in TGAudit. The following is a summary of the types of data available in the 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

For a complete list of available Collectors, please refer to **Appendix A**.

Collectors are required for defining new reports.

4.2. Reports

A Collector is the data source for a report. The following can be customized in a report definition:

- Specific columns
- Selection criteria – created using operation codes similar to SQL
- Field order
- Report Defaults to customize the data source collection – enables the report to run as efficiently as possible

Within TGAudit, there are over 200 built-in reports. Please refer to the **TGAudit Report Reference Guide** for detailed information on each report, details on why the report passed or failed in a built-in Report Card, as well as information on the report topic and recommendations on what to do to address existing vulnerabilities.

The four main areas of reports in TGAudit are:

1) Configuration Management
2) Network Management
3) Profile Management
4) Resource Management

4.3. Report Cards

Several reports can be grouped together in a single Report Card. When a Report Card is run, the reports defined within it are all run at the same time. A major benefit of Report Cards is the scoring capability that allows you to see a high-level pass/fail status for each individual report in the HTML output provided. Links to detailed reports will show additional information for any reports returning a failed status.

TGAudit provides built-in Report Cards mapped to the following compliance regulations:

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

5. Using TGAudit

5.1. Running Reports

There are several ways to run a report. Several menu options are built into the main menu for ease of access, as well as a “Work with Reports” interface to enable configuring and running reports, along with a TGRPT command interface to allow for scheduling and easy command line access.

5.1.1. TGAudit Menu Options

From the TGAudit Main Menu (TGMENU), select the menu option of the desired report. Reports can be found in submenus of options 1, 2, and 3, plus function keys of option 4 of the main menu.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                    More...
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

5.1.2. Work with Reports Interface

From the TGAudit Main Menu (TGMENU), select option 30 to “Work with Reports.” This will show you a list of all reports within TGAudit.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration
                  _
                                                                    More...
Selection or command
===> ____________________________________________________________________________
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

You can run any report by selecting option 7 on the desired report.

```
                              Work with Reports


 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID    Report Name
 _  Authority_List  Authorization List Details
 _  Authority_List  Authorization Lists with Public Access
 _  Controller_Atta Controllers and Attached Devices
 _  Controller_Desc Controller Description Details
 _  Device_Descript Device Descriptions - *APPC
 _  Device_Descript Device Description Details
 _  Exit_Points     Integrated File System Exits installed
 7  Exit_Points     Sockets-related Exit Points Not Secured
 _  Exit_Points     Unsecured Remote Server Exit Points
 _  IFS_Attributes  ASCII Files Stored in the IFS
 _  IFS_Attributes  Files Checked Out Status
 _  IFS_Attributes  IFS Directory Information
 _  IFS_Attributes  File Usage Information
 _  IFS_Attributes  Largest Files Report > 100Mb
 _  IFS_Attributes  Attributes for /QSYS.LIB                          +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

5.1.3. TGRPT Command Interface

From any TGAudit menu, press F18 to access the TG Run Report command (TGRPT) or, from the IBM i command line, type TGRPT and press F4.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                    More...
Selection or command
===>

F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

You will be prompted to input the relevant information to run the report.

```
                              TG - Run Report (TGRPT)

Type choices, press Enter.

Collector ID . . . . . . . . . .

                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

The Collector ID is a unique identifier for the data source of the report. Data sources for TGAudit reports are known as Collectors. To view a list of all Collectors available, please refer to **Appendix A**.

Press F4 on the Collector ID parameter to show the available data source collectors:

```
                    Specify Value for Parameter COLID

 Type choice, press Enter.

 Type . . . . . . . . . . . . . . :   CHARACTER
 Collector ID . . . . . . . . . . .   _______________________________

 Authority_List                         Job_Descriptions
 Controller_Attached_Devices            Job_Log_Details
 Controller_Description_Data            Job_Log_Summary
 Data_Area_Auditing                     Journal_AD
 Database_Auditing                      Journal_AF
 Device_Description_APPC                   :
 Device_Description_Data                   :
 Exit_Points                            Journal_ZC
 Field_Authority                        Journal_ZR
 IFS_Attributes                         Line_Description_Data
 IFS_Authorities                        Message_Queue
 IFS_Journaling                         Message_Queue_Data
 IFS_Status                             Network_Attributes                    +

 F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys
```

Type in the desired Collector ID and press Enter:

```
                    Specify Value for Parameter COLID

 Type choice, press Enter.

 Type . . . . . . . . . . . . . . :   CHARACTER
 Collector ID . . . . . . . . . . > User_Profiles_____________________

 Authority_List                         Job_Descriptions
 Controller_Attached_Devices            Job_Log_Details
 Controller_Description_Data            Job_Log_Summary
 Data_Area_Auditing                     Journal_AD
 Database_Auditing                      Journal_AF
 Device_Description_APPC                   :
 Device_Description_Data                   :
 Exit_Points                            Journal_ZC
 Field_Authority                        Journal_ZR
 IFS_Attributes                         Line_Description_Data
 IFS_Authorities                        Message_Queue
 IFS_Journaling                         Message_Queue_Data
 IFS_Status                             Network_Attributes                    +

 F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys
```

Once the data source collector is entered, press F4 on the Report ID parameter to show a list of available reports for that collector. Notice that the default Report ID for a Collector is either *NONE or *BASE. Using this default will run a report that is the base collection of all data available for the Collector without any specific report search criteria.

```
                    Specify Value for Parameter RPTID

Type choice, press Enter.

Type . . . . . . . . . . . . . :   CHARACTER
Report ID  . . . . . . . . . . .   *NONE

passwords_expired
passwords_expired_pwd
A*_Profiles
AllUsers
Enabled_IBM_Profiles
Not_used_90_days
Power_Users
Security_Officer
Users_JOBCTL
Users_Limit_Device
Users_PWDEXPITV
Users_SAVSYS


F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys
```

To run an existing report, type the desired Report ID from the list and press Enter.

```
                    Specify Value for Parameter RPTID

Type choice, press Enter.

Type . . . . . . . . . . . . . :   CHARACTER
Report ID  . . . . . . . . . . .   Power_Users

passwords_expired
passwords_expired_pwd
A*_Profiles
AllUsers
Enabled_IBM_Profiles
Not_used_90_days
Power_Users
Security_Officer
Users_JOBCTL
Users_Limit_Device
Users_PWDEXPITV
Users_SAVSYS


F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys
```

From the submittal screen, enter the desired output type:

```
                    Specify Value for Parameter OUTPUT

Type choice, press Enter.


Report output type . . . . . . .   *HTML___

  *
  *PRINT
  *OUTFILE
  *HTML
  *CSV
  *XML









F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys
```

Once all parameters are entered, press Enter to run the report.

```
                            TG - Run Report (TGRPT)

Type choices, press Enter.

Collector ID . . . . . . . . . . > User_Profiles                    
Collector Name . . . . . . . . .   'User Profile Information'


Report ID  . . . . . . . . . . . > Power_Users                      
User profile . . . . . . . . . .   *ALL_____      Name, generic*, *ALL
Override report defaults?  . . .   *NO_           *YES, *NO
Reload collector data  . . . . .   *AI_           *AI, *YES, *NO
Report output type . . . . . . . > *HTML___       *, *PRINT, *OUTFILE, *HTML...
Run interactively? . . . . . . .   Y___           *YES, *NO





                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

To view report output, ensure NetServer has been configured (see Chapter 3. Configuration) to automatically display HTML, CSV, and XML output that will be stored in the configured IFS folder. Alternatively, view data on the screen, in a spooled file, or a basic output file.

5.2. Running Report Cards

There are several ways to run a Report Card. Several menu options are built into the main menu for ease of access, as well as a "Work with Report Cards" interface to enable configuring and running Report Cards, along with a TGCARD command interface to allow for scheduling and easy command line access.

5.2.1. TGAudit Menu Options

From the TGAudit Main Menu (TGMENU), select option 10 to access Regulation Report Cards and select the menu option of the desired Report Card.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                    More...
Selection or command
===> ____________________________________________________________________________

F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

5.2.2. Work with Report Cards Interface

From the TGAudit Main Menu (TGMENU), select option 31 to “Work with Report Cards.” This will show you a list of all Report Cards within TGAudit.

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                    More...
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

You can run any report by selecting option 7 on the desired Report Card.

```
                            Work with Report Cards


 2=Change   3=Copy   4=Delete   7=Run   9=Select Reports

Opt Report Card ID       Report Card                            Category
 _  FISMA                Federal Information Security Management Regulations
 _  GLBA                 Gramm-Leach-Bliley Act                 Regulations
 7  HIPAA                Health Insurance Portability and Accoun Regulations
 _  IFS_Reports          Integrated File System Reports         IFSReports
 _  ISO_27001            Information security management system  Regulations
 _  PCI                  PCI DSS 3.1                            Regulations
 _  PCI_20               PCI DSS 2.0                            Regulations
 _  Security_Assessment  TGFree Security Assessment             Analysis
 _  SOX                  Sarbanes-Oxley                         Regulations
 _  STDAUS               Standard Australia                     Regulations




 F1=Help   F3=Exit   F6=Add Report Card    F12=Cancel
```

5.2.3. TGCARD Command Interface

From any TGAudit menu, press F19 to access the TG Run Report Card (TGCARD) command or, from the IBM i command line, type TGCARD and press F4. You will be prompted to input the relevant information to run the Report Card.

```
                          TG - Run Report Card (TGCARD)

 Type choices, press Enter.

 Report Card Id . . . . . . . . . . > PCI                              
 Report Card Name . . . . . . . .   'PCI DSS 3.1'


 Category . . . . . . . . . . . . .   Regulations                      
 User profile . . . . . . . . . . .   *ALL        Name, generic*, *ALL
 Object . . . . . . . . . . . . . .   *ALL        Name, generic*, *ALL
   Library  . . . . . . . . . . . .     QGPL       Name, *ALL
 Starting date and time::
   Starting date  . . . . . . . . .   *CMS        Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . . .   *          Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . . .   *CUR        Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . . .   *          Time (hhmmss)


                                                                      More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

5.3. Managing Report and Report Card History

From any TGAudit menu, press F20 to “Work with Report History” to see details about reports and Report Cards that have been run on the system.

```
                          Work with Report History


  5=Run details   7=Re-run   8=Last Run Results
                                                  Run     Out    Run
Opt Report ID                   Collector ID     Status  Type   Timestamp
 _  Authority_List_Details      Authority_List   *END    *      2016-03-17-23.25.18
 _  Authority_List_Public       Authority_List   *END    *      2016-03-17-23.22.03
 _  Authority_List_Details      Authority_List   *END    *      2016-03-17-20.04.47
 _  AllUsers                    User_Profiles    *END    *      2016-03-16-04.31.56
 _  QAUDLVL_CREATE              System_Values    *END    *      2016-03-16-04.28.54
 _  QAUDLVL_OBJMGT              System_Values    *END    *_     2016-03-16-04.28.04
 _  *BASE                       Journal_OM       *END    *      2016-03-16-04.23.07
 _  *BASE                       Journal_OR       *END    *      2016-03-16-04.21.48
 _  *BASE                       Journal_DO       *END    *      2016-03-16-04.21.06
 _  *BASE                       Journal_CO       *END    *      2016-03-16-04.20.12
 _  CMP20002F_TGPROD            Database_Auditi  *END    *      2016-03-10-22.09.30
 _  CMP20002F_QGPL              Database_Auditi  *END    *      2016-03-10-22.08.00
 _  *ALL_QGPL                   Database_Auditi  *END    *      2016-03-10-22.06.36
 _  *BASE                       Journal_PW       *END    *      2016-03-10-20.09.53
 _  Job_Descriptions_Libl       Job_Description  *END    *      2016-03-10-19.11 +

 F1=Help   F3=Exit   F12=Cancel
```

5 = Run Details

View run details such as Job Name, Job User, Job Number, Job Status, Start Time, End Time, Run Type, Client IP and Server IP.

7 = Re-run

Run the report or Report Card again, using the same submittal parameters.

8 = Last Run Results

View the report results if the report output select was *XML, *HTML or *CSV (Excel).

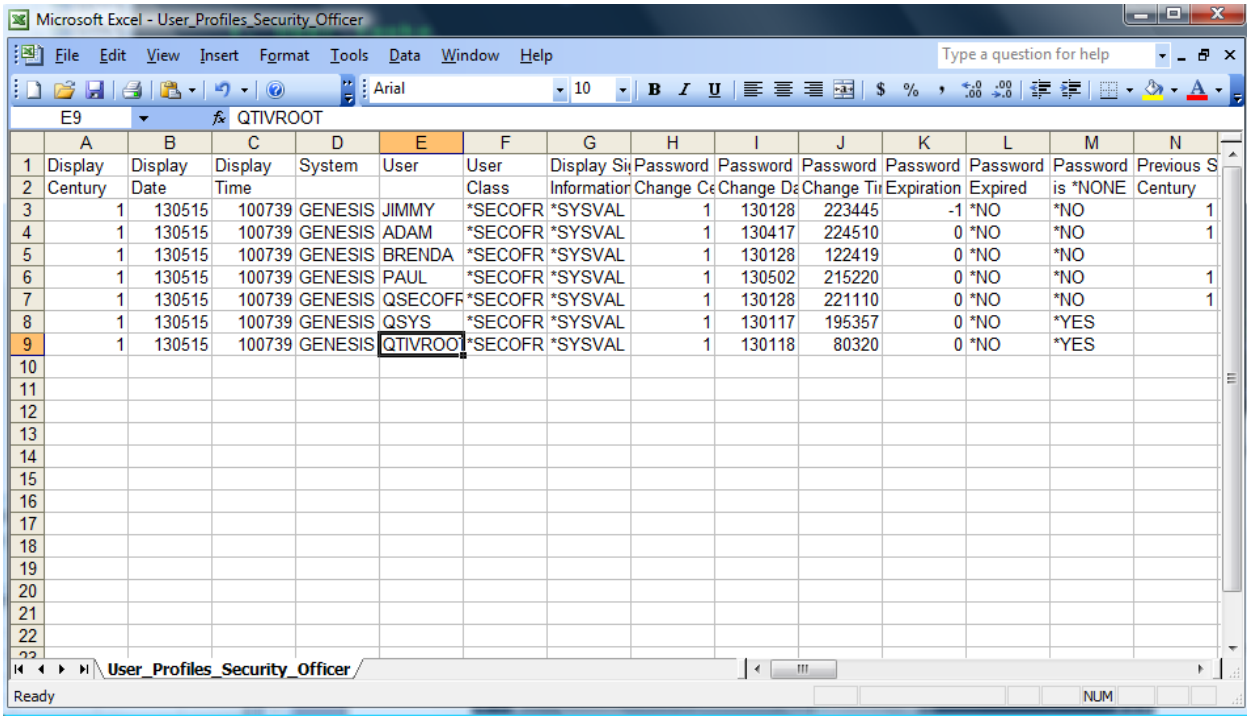
5.4. Report Output Types

For your convenience, all reports and Report Cards have multiple output options:

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

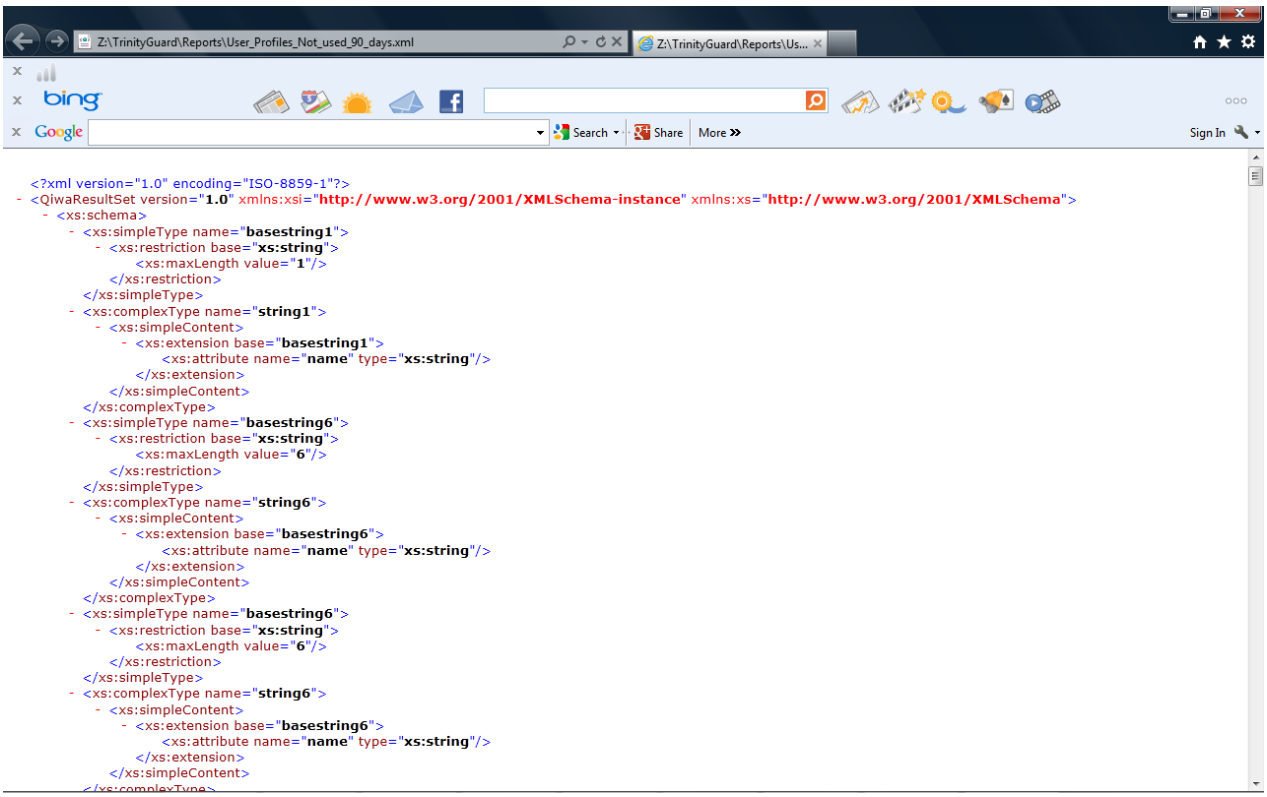
HTML is the recommended output type since it takes advantage of the most user-friendly data layouts available. If you run a report from a client with an internet browser and have configured NetServer (as per Chapter 3. Configuration), the report will display automatically.

5.4.1. Preview of CSV format



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

5.4.2. Preview of XML format




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

5.4.3. Preview of HTML format

PCI DSS 3.1

[redacted] | [redacted] | [redacted] | 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	
2.2.C	Resources	System Security Audit Journal Exists	0	PASS	Detailed Report	
5.1	Resources	Integrated File System Security	1	FAIL	Detailed Report	
2.2.C	Configuration	System, User, and Object Auditing Control Configuration	0	PASS	Detailed Report	
10.2	Configuration	Attention Events are Audited	0	PASS	Detailed	

5.4.4. Detail views

From a Report Card in HTML, click on the Detailed Report hyperlink to see detailed information for a report.

Sample detailed report:

Enabled IBM Profiles For User: *ALL

[redacted] | [redacted] | [redacted] | 14:05:10

Display Century	Display Date	Display Time	System	User	User Class	Display Sign-on Information	Password Change Century	Password Change Date	Password Change Time	Password Expiration Interval	Password Set Expired	Password is *NONE	Previous Sign-on Century	Previous Sign-on Date
1	160318	140510	TGDEV3	QANZAGENT	*SYSOPR	*NO	1	160215	182502	0	*NO	*YES		
1	160318	140510	TGDEV3	QAUTPROF	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QBRMS	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QCLUSTER	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QCOLSRV	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDBSHR	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDBSHRDO	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDFTOWN	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDIRSRV	*USER	*NO	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDLFM	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDOC	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QDSNX	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		
1	160318	140510	TGDEV3	QEJB	*USER	*SYSVAL	1	160215	182501	0	*NO	*YES		

5.4.5. Report Help

Click on the symbol to view online help specific to a report. The following is a sample help page:

Remote server exit points not secured - help

This report evaluates whether or not exit programs are installed on remote server exit points.

PASS = Exit programs are installed on remote server exit points.

FAIL = Exit programs are NOT installed on all remote server points.

Communication for ODBC, FTP, and TELNET transactions, along with transactions for numerous other remote servers such as RMTCMD, DDM, etc… pass through remote server exit points. Exit programs can be installed on remote server exit points to monitor and secure transactions. It is important to know who is accessing the data on your system so you can verify if the access is authorized or not.

While it is best to implement object-level and Integrated File System (IFS) security to protect your system, sometimes, due to application limitations, it may not be possible to implement this type of security effectively and an application may break if object-level security is implemented. In a situation like this, it is recommended you monitor all your remote connections and the data access. Remote server exit points are your only option in these scenarios.

At a minimum, it is recommended to have exit point programs monitoring your remote server exit points so you can review who is accessing your data.

5.5. What do I do next?

TGAudit Reports and Report Cards may highlight some areas of concern if your system has not been properly secured. Once you are aware of these vulnerabilities, the next step is to rectify any issues found. You can click on the help symbol on any report to get more information and to help you better understand 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@netiq.com.

6. Job Activity Monitor

The Job Activity Monitor is a comprehensive component of TGAudit that provides detailed viewing into job activity of interactive user and batch jobs running on the system. This type of monitoring is useful for auditing activity on the system for highly-privileged users with access to sensitive information or critical batch processing of sensitive jobs to help ensure system integrity.

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

To access the Job Activity Monitor Menu, select option 3 from the TGAudit Main Menu:

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                      More...
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

```
TGMJOBLOG                    Job Activity Monitor Menu

Select one of the following:

     1. Work with Job Activity
     2. Job Activity Summary Report
     3. Job Activity Details Report

    10. Work with Activity Monitor Rules
    11. Work with Groups
    12. Work with Monitored Subsystems
    13. Work with Monitored Commands

    20. Job Activity Archival



                                                                       Bottom
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

6.1. Configure Job Activity Monitoring

6.1.1. Configure Batch Jobs

To monitor activity for batch jobs, the subsystem where the jobs will run must be added in the “Work with Monitored Subsystems” screen.

Select option 12 from the Job Activity Monitor Menu to access the “Work with Monitored Subsystems” screen:

```
                                   Work with Monitored Subsystems



                                                                   Position to: _________
1=Enable  2=Disable  4=Delete  10=Work with Job Activity

    Subsystem  Subsystem                                                                  Log
OPT Name       Library    Subsystem Description                                           Status

__  QBATCH     QSYS       Batch Subsystem                                                 *ENABLED









                                                                                            Bottom
F1=Help  F3=Exit  F6=Add  F8=Work with Activity Monitor Rules  F9=Job Activity Summary Report
F10=Job Activity Details Report  F11=Work with Job Activity(All Subsystems)  F12=Cancel
```

To add the desired subsystem to monitor, press F6 and enter the subsystem name, library, and log status. Once it is added, you can enable or disable activity monitoring for a subsystem by editing the Log Status of the subsystem. Activity for a subsystem will only be monitored if the Log Status is set to *ENABLED.

```
                                   Add Subsystem





Subsystem name  . . . . : QBATCH___

    Subsystem Library . . . : QSYS_____


Subsystem Description . :

    Log Status  . . . . . . : *ENABLED__   (*ENABLED, *DISABLED)









F1=Help  F3=Exit  F12=Cancel
```

6.1.2. Configure Interactive Jobs

For interactive jobs, four commands can be configured to monitor interactive job activity: ENDJOB, SIGNOFF, ENDJOBABN, and ENDPASTHR. You can specify one or all of these commands to be monitored. To ensure the most accurate monitoring of interactive user jobs, it is recommended to configure all four commands. User activity is captured at the time a job ends through one of the four commands.

Select option 13 from the Job Activity Monitor Menu to access the "Work with Monitored Commands" screen:

```
                                   Work with Monitored Commands

                                                                  Position to: _________
4=Delete

        Command         Command
OPT     Name            Library         Description

 _      ENDJOB          QSYS            End Job
 _      SIGNOFF         QSYS            Sign Off

                                                                                   Bottom
F1=Help  F3=Exit  F6=Add  F8=Activity Monitor Rules
F9=Job Activity Summary Report  F10=Job Activity Details Report  F12=Cancel
```

To add the desired command to monitor, press F6 and enter the command name and library.

```
                                   Add Monitored Command

Command Name  . . . . . : ENDPASTHR

    Command Library . . . . : QSYS

Description   . . . . . : End Pass-Through

F1=Help  F3=Exit  F12=Cancel
```

6.1.3. Configure Activity Monitor Rules

Once the desired subsystems are added to monitor activity, rules must be set up to configure the desired logging levels of the particular users that will be monitored. By default, a *PUBLIC rule exists in the "Work with Activity Monitor Rules" screen that applies to all job users. This default rule will not log any activity for *PUBLIC.

```
                                    Work with Activity Monitor Rules



2=Edit 4=Delete


OPT      User/Group       Level      Severity      Text            Log CL

_        *PUBLIC          0          99            *NOLIST         *NO
_        :OPERATORS       4          00            *SECLVL         *YES
_        :TELLERS         3          00            *SECLVL         *NO
_        QSECOFR          4          00            *SECLVL         *YES









                                                                                                  Bottom
F1=Help  F3=Exit  F6=Add  F12=Cancel
```

To add a new rule for activity monitoring, press F6 and enter the desired user and logging levels:

```
                                 Work with Activity Monitor Rules - Add Record



User/Group ......: PWRUSER    (User Name, :Group)


           Message Logging  :

                   Level      4

                   Severity   00

                   Text       *SECLVL


           Log CL commands  : *YES




F1=Help  F3=Exit  F12=Cancel
```

6.1.3.1. Working with User Groups to Simplify Activity Monitor Rules

In addition to monitoring individual users, you can help ease rule management by creating user groups. User groups are created through option 11, “Work with Groups,” from the Job Activity Monitor Menu. 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 access the “Work with User Groups” screen, select option 11 from the Job Activity Monitor Menu.

```
TGMJOBLOG                    Job Activity Monitor Menu

Select one of the following:

     1. Work with Job Activity
     2. Job Activity Summary Report
     3. Job Activity Details Report

    10. Work with Activity Monitor Rules
    11. Work with Groups
    12. Work with Monitored Subsystems
    13. Work with Monitored Commands

    20. Job Activity Archival

                                                                    Bottom
Selection or command
===>

F3=Exit          F4=Prompt    F9=Retrieve    F12=Cancel    F17=TG Management
F18=Run Report   F19=Run Rpt Card           F20=Report History
```

To create a new group, press F6.

```
                                   Work with User Groups


2=Edit 4=Delete 10=Work with Users

Subset Criteria  -  Grp Name: *ALL        Grp Desc.: *ALL

                                                          Position to:

OPT   Group Name    Group Description


                                                  (Sort by group name ascending seq.)
F1=Help  F3=Exit  F6=Add  F8=Subset  F10=Sort  F12=Cancel
```

Enter the name and description of the group. The group name must begin with a colon (:).

```
                                   Work with User Groups - Add Record




Group Name . . . : :OPERATORS

Group Description: Operations Group_________________________________________________________________________________

F1=Help  F3=Exit  F12=Cancel
```

Once the group is created, you can add users to the group. These are the users a rule will be applied to when the group name is used in creating an activity monitor rule. Select option 10 next to the group you desire to add users to and press Enter.

```
                                   Work with User Groups


2=Edit 4=Delete 10=Work with Users

Subset Criteria  -  Grp Name: *ALL        Grp Desc.: *ALL

                                                                          Position to: _________
OPT   Group Name    Group Description
10    :OPERATORS    Operations Group


                                                                                                Bottom
                                                              (Sort by group name ascending seq.)
F1=Help  F3=Exit  F6=Add  F8=Subset  F10=Sort  F12=Cancel
User Group :OPERATORS added successfully.
```

Press F6 on the “Work with Users” screen to add users.

```
                                        Work with Users

Group Name.......: :OPERATORS
Group Description: Operations Group

2=Edit 4=Delete                                                    Position to: _________

OPT  User Name   User Description                                                   Exist on
                                                                                    Server

                                                                 (Sort by user name ascending seq.)
F1=Help  F3=Exit  F6=Add  F10=Sort  F12=Cancel
```

Enter the user name and description and press Enter.

```
                                    Work with Users  -  Add Record

Group Name . . . . : :OPERATORS
Group Description .: Operations Group

User  Name . . . . : SMITHJ   

User Description . : John Smith                                                                  

Exists on Server . : *YES

F1=Help  F3=Exit  F12=Cancel
Press ENTER to confirm adding user or F12 to CANCEL.
```

Now, users can simply be added or removed to the group as needed, without having to alter the main activity monitor rule.

```
                                        Work with Users

Group Name.......: :OPERATORS
Group Description: Operations Group

2=Edit 4=Delete                                                    Position to: _________

OPT  User Name   User Description                                                    Exist on
                                                                                     Server
__   CARLISLEK   Ken Carlisle                                                          *YES
__   GROVESA     Amy Groves                                                            *YES
__   LOWMANS     Susan Lowman                                                          *YES
__   SMITHJ      John Smith                                                            *YES

                                                                                        Bottom
                                                          (Sort by user name ascending seq.)
F1=Help  F3=Exit  F6=Add  F10=Sort  F12=Cancel
```

6.1.4. Viewing Job Activity

From the Job Activity Monitor Menu, there are three options that allow you to view job activity.

```
TGMJOBLOG                    Job Activity Monitor Menu

Select one of the following:

     1. Work with Job Activity
     2. Job Activity Summary Report
     3. Job Activity Details Report

    10. Work with Activity Monitor Rules
    11. Work with Groups
    12. Work with Monitored Subsystems
    13. Work with Monitored Commands

    20. Job Activity Archival

                                                                    Bottom
Selection or command
===> _
F3=Exit          F4=Prompt    F9=Retrieve    F12=Cancel    F17=TG Management
F18=Run Report   F19=Run Rpt Card           F20=Report History
```

6.1.4.1. Option 1. Work with Job Activity

Use option 1 from the Job Activity Monitor Menu to view job details of monitored jobs. To change the columns the screen is sorted on, position your cursor to the column header and press F10. The columns being sorted on are displayed in white.

```
                                   Work with Job Activity

4=Delete 5=Display                                                          Position to: _________

Subset Criteria - Subsystem . . .: *ALL                Job Name . . : *ALL        Number: *ALL    User: *ALL
                  Start Date/Time:                     End Date/Time:

OPT    Job Name       Job Number     Job User       Start Date  Start Time     End Date    End Time       Subsystem

 _     QPADEV0003     003445         KAPILA         2016-03-18  01:37:05       2016-03-18  02:24:13       QSYS/QINTER
 _     QPADEV0002     003444         KAPILA         2016-03-18  01:35:56       2016-03-18  02:24:20       QSYS/QINTER
 _     QPADEV0007     003442         PMB            2016-03-18  00:10:56       2016-03-18  00:12:38       QSYS/QINTER
 _     QDFTJOBD       003420         ARP            2016-03-17  16:24:03       0001-01-01  00:00:00       QSYS/QBATCH
 _     QPADEV0002     003415         KAPILA         2016-03-17  08:50:35       2016-03-17  08:51:29       QSYS/QINTER
 _     QPADEV0002     003334         KAPILA         2016-03-16  10:33:44       2016-03-16  12:21:06       QSYS/QINTER
 _     QPADEV0002     003243         KAPILA         2016-03-13  01:13:55       2016-03-13  03:10:19       QSYS/QINTER
 _     QPADEV0004     003208         KAPILA         2016-03-11  21:07:43       2016-03-12  01:17:10       QSYS/QINTER
 _     QPADEV0002     003204         ARP1           2016-03-11  17:44:38       2016-03-11  17:45:06       QSYS/QINTER
 _     QPADEV0004     003194         KAPILA         2016-03-11  06:47:50       2016-03-11  07:04:22       QSYS/QINTER
 _     QPADEV0002     003193         KAPILA         2016-03-11  06:46:38       2016-03-11  07:04:29       QSYS/QINTER
 _     QPADEV0002     003185         KAPILA         2016-03-11  01:23:06       2016-03-11  01:43:06       QSYS/QINTER
                                                                                                                More...

F1=Help  F3=Exit  F8=Subset  F10=Sort  F12=Cancel
```

You can also subset the data shown on the “Work with Job Activity” screen by pressing F8 and entering the values you are searching for. This will narrow the scope of data show on the screen to what fits your subset criteria. The Subset Criteria is displayed at the top of the “Work with Job Activity” screen.

To display details of a job, select option 5 next to the desired job name. The following screen will be displayed and option 5 can be selected again to display even further detail about each message available in the job activity.

```
                                    Work with Job Activity - Detail


Subsystem : QSYS/QINTER            Job . . . : 015036/PMB/QPADEV0002

5=Display MSG Data

Opt  Msg      Msg       Msg        Msg        Msg      Msg
     ID       Sev       Type       Date       Time     Data
 _   CPF1124 000000000 *INFO      2016-05-27 12:12:16 Job 015036/PMB/QPADEV0002 started on 05/27/16 at 12:12:16 in subsystem QINT
 _   CPI9808 000000010 *INFO      2016-05-27 12:12:16 Model file QAMHJLPR in library QSYS used for output file.
 _   CPI9802 000000020 *INFO      2016-05-27 12:12:16 Record format for file CMP20020F in TGDATA does not match model file.
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:16 6800 - RRTJOB RTGDTA(*ANY)
 _   *IMMED  000000000 *RQS       2016-05-27 12:12:52 tgmenu
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:52 301 - RTVJOBA JOB(&DEV)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:52 1000 - GO MENU(TGMENUD)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:53 1600 - RTVNETA SYSNAME(&SYSNAME)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:53 1700 - RTVJOBA JOB(&JOB) CURUSER(&CURUSER) TYPE(&TYPE) DATETIME(&DATETIME)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:53 6700 - RTVAUTLE AUTL(TGAUTL) USER(PMB) EXCLUDE(&EXCLUDE)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:53 8000 - RTVUSRPRF USRCLS(&USRCLS)
 _   *IMMED  000000000 *CMD       2016-05-27 12:12:53 - RETURN        /* RETURN due to end of CL program */
                                                                                                                      More...

F1=Help  F3=Exit  F12=Cancel  F17=Top  F18=Bottom
```

6.1.4.2. Option 2. Job Activity Summary Report

Use option 2 from the Job Activity Monitor Menu to generate a report of job activity summary information similar to what is shown on the main “Work with Job Activity” screen.

```
                                TG - Run Report (TGRPT)

 Type choices, press Enter.

 Collector ID . . . . . . . . . . > Job_Activity_Summary
 Collector Name . . . . . . . . .   'Job Activity Summary'
 Report ID  . . . . . . . . . . . > *NONE          Name, Job_Activity_Summary...
 User profile . . . . . . . . . .   *ALL           Name, generic*, *ALL
 Starting date and time::
   Starting date  . . . . . . . .   *CUR           Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . .   _________       Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . .   *CUR           Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . .   _________       Time (hhmmss)
 Override report defaults?  . . .   *NO            *YES, *NO
 Report output type . . . . . . > *HTML___         *, *PRINT, *OUTFILE, *HTML...
 Run interactively? . . . . . . > *YES             *YES, *NO



                                                                            Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

User profile – Enter the user name you wish to gather data for. Valid values are a specific user profile, a generic user name (ex: SMITH* to report on user names that begin with SMITH), or *ALL to report on all available users.

Starting date - Enter specific date or one of the special dates below.

Starting time - Enter specific time.

Ending date - Enter specific date or you may enter one of the special dates below.

Ending time - Enter specific time.

Special Date Values	
*CUR	Current day
*CMS	Current month start
*LMS	Last month start
*LME	Last month start
*LYS	Last year start
*LYE	Last year end
*LWS	Last week start (current date minus 7 days)
*LDS	Last day start

Override report defaults? - *YES or *NO.
If you have set defaults for this report in the "Work with Reports" screen (TGMENU – Option 30), you can select whether or not you want to override those values by entering *YES or retaining the report defaults by selecting *NO.

Report output type – Specify the type of report output to be generated.
Valid values are:
* - generates report output to the display screen
*PRINT – generates report output to a printer file
*HTML – generates report output to an HTML file that will be automatically displayed if run interactively. HTML reports are stored in the TrinityGuard IFS folder.
*CSV – generates report data to a .csv file that is stored in the TrinityGuard IFS folder. This output option is useful for manipulating data through MS Excel.
*XML – generates report date to a .xml file that is stored in the TrinityGuard IFS folder.

Run interactively? – Specify *YES to run interactively or *NO to run the report in batch.

6.1.4.3. Option 3. Job Activity Details Report

Use option 3 from the Job Activity Monitor Menu to generate a report of detailed job log information for monitored jobs.

```
                              TG - Run Report (TGRPT)

 Type choices, press Enter.

 Collector ID . . . . . . . . . . . > Job_Activity_Details
 Collector Name . . . . . . . . . .   'Job Activity Details'
 Report ID  . . . . . . . . . . . . > Job_Activity_Details
 User profile . . . . . . . . . . .   *ALL_______     Name, generic*, *ALL
 Starting date and time::
   Starting date  . . . . . . . . .   *CUR______     Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . . .   ________       Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . . .   *CUR______     Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . . .   ________       Time (hhmmss)
 Override report defaults?  . . .   *NO_            *YES, *NO
 Report output type . . . . . . . > *HTML___        *, *PRINT, *OUTFILE, *HTML...
 Run interactively? . . . . . . . > *YES            *YES, *NO



                                                                          Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

User profile – Enter the user name you wish to gather data for. Valid values are a specific user profile, a generic user name (ex: SMITH* to report on user names that begin with SMITH), or *ALL to report on all available users.

Starting date - Enter specific date or one of the special dates below.

Starting time - Enter specific time.

Ending date - Enter specific date or you may enter one of the special dates below.

Ending time - Enter specific time.

Special Date Values	
*CUR	Current day
*CMS	Current month start
*LMS	Last month start
*LME	Last month start
*LYS	Last year start
*LYE	Last year end
*LWS	Last week start (current date minus 7 days)
*LDS	Last day start

Override report defaults? - *YES or *NO.
If you have set defaults for this report in the "Work with Reports" screen (TGMENU – Option 30), you can select whether or not you want to override those values by entering *YES or retaining the report defaults by selecting *NO.

Report output type – Specify the type of report output to be generated.
Valid values are:
* - generates report output to the display screen
*PRINT – generates report output to a printer file
*OUTFILE – generates report output to an output file. You will be prompted to enter the output file name and

library.
*HTML – generates report output to an HTML file that will be automatically displayed if run interactively. HTML reports are stored in the TrinityGuard IFS folder.
*CSV – generates report data to a .csv file that is stored in the TrinityGuard IFS folder. This output option is useful for manipulating data through MS Excel.
*XML – generates report date to a .xml file that is stored in the TrinityGuard IFS folder.

Run interactively? – Specify *YES to run interactively or *NO to run the report in batch.

6.1.5. Archiving Job Activity Data

Since job activity data is very detailed, it can accumulate in large quantities very quickly and you may need to manage storage by archiving the data. The TGJOBACTA command allows you to do this.

```
                    TG Job Activity Archival (TGJOBACTA)

 Type choices, press Enter.

 Starting date and time::
   Starting date  . . . . . . . .   *CUR        Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . .   _________   Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . .   *CUR        Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . .   _________   Time (hhmmss)
 Delete data after archive  . . .   *NO         *YES, *NO
 Archive Type . . . . . . . . . .   *OUTFILE    *SAVF, *OUTFILE
 Archive File . . . . . . . . . .   *NONE       Name, *NONE
   Library  . . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
 Replace or add records . . . . .   *REPLACE    *REPLACE, *ADD
 Run interactively? . . . . . . .   *NO         *YES, *NO
 Job queue  . . . . . . . . . . .   QBATCH      Name, *NONE
   Library  . . . . . . . . . . .     *LIBL     Name, *LIBL, *CURLIB
 Schedule?  . . . . . . . . . . .   *NO         *YES, *NO

                                                                      Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Starting date - Enter specific date or one of the special dates below.

Starting time - Enter specific time.

Ending date - Enter specific date or you may enter one of the special dates below.

Ending time - Enter specific time.

Special Date Values	
*CUR	Current day
*CMS	Current month start
*LMS	Last month start
*LME	Last month start
*LYS	Last year start
*LYE	Last year end
*LWS	Last week start (current date minus 7 days)
*LDS	Last day start

Delete data after archive
*YES – TGAudit Job Activity data is deleted after the data is saved to archive.
*NO – TGAudit Job Activity data remains after being archived.

Archive Type
*SAVF – TGAudit Job Activity data will be saved to an archive save file.
*OUTFILE – TGAudit Job Activity data will be saved to an output file.

Archive File
Specify the name of the save file or output file where TGAudit Job Activity data will be archived.

Library
Specify the library name where the save file or output file exists.

Run interactively?
*YES – Executes the TGJOBACTA command interactively.
*NO – Submits the TGJOBACTA command to run in batch.

Job Queue
Specify the job queue in which the job will run. This parameter is only valid for batch jobs.

Job Queue Library
Specify the library where the job queue resides. This parameter is only valid for batch jobs.

Schedule?
*YES – The job is scheduled using IBM's job scheduler. The default job name given is TGJOBACTA. IBM job scheduler options are displayed and can be edited as desired.
*NO – The job is not scheduled.

7. Authority Collection

Authority Collection is a security feature IBM introduced to the operating system in IBM i 7.3. When activated, it collects the minimum required authorities and users' current authorities to the objects they access. The information can be used to determine the authorities required for an application to run and help eliminate unnecessary over-authorization.

TGAudit 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 Authority Collection, select option 4 from the TGAudit Main Menu:

```
TGMENUD                          TGAudit - Main Menu

Select one of the following:

   Reporting:
     1. Security and Configuration Reports
     2. Data Level Reports
     3. Job Activity Monitor
     4. Authority Collection

    10. Regulation Report Cards

   Management:
    30. Work with Reports (TGWRKRPT)
    31. Work with Report Cards (TGWRKCARD)
    32. Audit Configuration

                                                                        More...
Selection or command
===> _
F3=Exit          F4=Prompt   F9=Retrieve   F12=Cancel   F17=TG Management
F18=Run Report   F19=Run Rpt Card          F20=Report History
```

Any users on the system that have been enrolled in Authority Collection will be displayed on this screen. You can also quickly see if Authority Collection is currently active for a user and if an authority collection repository exists for the user.

```
                                        Work with Authority Collection Users


3=End Collection 4=Delete Collection 5=Display Collection Details


OPT      User            Collection     Repository
                         Active         Exists

 _       ARP             YES            YES
 _       ARTURO          YES            YES
 _       ARTUROL         YES            YES
 _       AVG             YES            YES
 _       LOWLOW          YES            YES
 _       XXTEST1         YES            YES
 _       XXTEST2         YES            YES
 _       XXTEST3         NO             YES
 _       XXTEST4         YES            YES
 _       XXTEST5         YES            YES


                                                                                                                Bottom
F1=Help  F3=Exit  F6=Start Collection  F9=Auth Col IFS Report  F10=Auth Col Native Report  F12=Cancel
```

3 = End Collection
This option allows you to stop collecting authority information for the specified user.

4 = Delete Collection
This option allows you to delete the repository that was created for the user to collect authority information. Authority Collection must be ended for the user prior to deleting the collection.

5 = Display Collection Details
This option displays the values Authority Collection was started with for the specified user. For example:

```
                                        Display Collection Details


User Profile . . : XXTEST5      Collection Active: YES       Repository Exists . : YES

STRAUTCOL values :

Library  . . . . : QSYS
  ASP device  . .: *SYSBAS

Object . . . . . : *ALL

Object type  . . : *ALL

Include DLO  . . : *NONE

Include file
   system objects: *NONE

Delete collection: *NO

Detail . . . . . : *OBJINF

F1=Help  F3=Exit  F12=Cancel
```

F6=Start Collection

Displays the IBM Start Authority Collection (STRAUTCOL) command and allows you to begin collecting authority collection information for the specified user.

```
                    Start Authority Collection (STRAUTCOL)

 Type choices, press Enter.

 User profile . . . . . . . . . . .   _________     Name
 Library and ASP device:          _
   Library  . . . . . . . . . . . .   __________    Name, *NONE, *ALL
   ASP device . . . . . . . . . . .   *SYSBAS   _   Name, *SYSBAS
                 + for more values _
 Object . . . . . . . . . . . . . .   *ALL      _   Name, generic*, *ALL
                 + for more values    __________
 Object type  . . . . . . . . . . .   *ALL   __     *ALL, *CMD, *DTAARA...
                 + for more values    _______
 Include DLO  . . . . . . . . . . .   *NONE         *NONE, *ALL, *DOC, *FLR
                                      _____
 Include file system objects  . . .   *NONE __       *NONE, *ALL, *BLKSF...
                 + for more values    _______
 Delete collection  . . . . . . . .   *NO _         *NO, *YES
 Detail . . . . . . . . . . . . . .   *OBJINF       *OBJINF, *OBJJOB

                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

F9=Auth Col IFS Report

Allows you to run the Authority Collection report for objects in the Integrated File System (IFS). In order for data to show on the IFS report, there must be users enrolled in Authority Collection that have values specified on the "Include DLO" and/or "Include file system objects" parameters. To verify if a user has values specified for these parameters, select Option 5 to Display Collection Details next to the desired user and press Enter.

```
                          TG - Run Report (TGRPT)

 Type choices, press Enter.

 Collector ID . . . . . . . . . . > Authority Collection
 Collector Name . . . . . . . . . > 'Authority Collection Data'
 ____________________________________________________________________________
 _______
 Report ID  . . . . . . . . . . . > Authority IFS
 User profile . . . . . . . . . . > *ALL      _    Name, generic*, *ALL
 Starting date and time::
   Starting date  . . . . . . . . > *CUR      _    Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . .   ________       Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . . > *CUR      _    Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . .   ________       Time (hhmmss)
 Override report defaults?  . . .   *NO _          *YES, *NO
 Reload collector data  . . . . .   *AI _          *AI, *YES, *NO
 Report output type . . . . . . . > *HTML __       *, *PRINT, *OUTFILE, *HTML...
 Run interactively? . . . . . . . > *YES           *YES, *NO
                                                                        Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

F10=Auth Col Native Report

Allows you to run the Authority Collection report for native objects in the QSYS.LIB file system. In order for data to show on the Native Report, there must be users enrolled in Authority Collection that have values specified on the "Object" parameter. To verify if a user has values specified for these parameters, select Option 5 to Display Collection Details next to the desired user and press Enter.

```
                              TG - Run Report (TGRPT)

 Type choices, press Enter.

 Collector ID . . . . . . . . . . > Authority Collection
 Collector Name . . . . . . . . . > 'Authority Collection Data'
 ________________________________________________________________________________
 ________
 Report ID  . . . . . . . . . . . > Authority Objects
 User profile . . . . . . . . . . > *ALL        Name, generic*, *ALL
 Starting date and time::
   Starting date  . . . . . . . . > *CUR        Date, *LMS, *LME, *LYS, *LYE..
   Starting time  . . . . . . . .   ________     Time (hhmmss)
 Ending date and time::
   Ending date  . . . . . . . . .   *CUR        Date, *LMS, *LME, *LYS, *LYE..
   Ending time  . . . . . . . . .   ________     Time (hhmmss)
 Override report defaults?  . . .   *NO         *YES, *NO
 Reload collector data  . . . . .   *AI         *AI, *YES, *NO
 Report output type . . . . . . . > *HTML       *, *PRINT, *OUTFILE, *HTML...
 Run interactively? . . . . . . . > *YES        *YES, *NO
                                                                          Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

8. Regulation Report Cards

This chapter provides some background information regarding common compliance regulations that are standard requirements for many companies. The built-in Report Cards in TGAudit help users decipher these complex compliance regulation requirements specifically for the IBM i platform and allow you to quickly gather data to start evaluating your system.

To access the Report Cards that have pre-defined mappings to standard compliance regulations, select option 10 from the TGAudit Main Menu (TGMENU) for Regulation Report Cards.

```
TGMREG                        Regulation Report Cards

Select one of the following:

     1. Payment Card Industry Data Security Standard (PCI DSS)
     2. Health Insurance Portability and Accountability Act (HIPAA)
     3. Sarbanes Oxley Act (SOX)
     4. Gramm-Leach-Bliley Act (GLBA)
     5. Federal Information Security Management Act of 2002 (FISMA)
     6. Standard Australia
     7. Information security management system Standard (ISO 27001)

                                                                    Bottom
Selection or command
===>
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F19=Run Rpt Card
F20=Report History
```

8.1. 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.

Sample data:

PCI DSS 3.1

TGDEV2 PMB 2016-05-25 14:26:45

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	0	PASS	Detailed Report	
1.1.5B	Network	Server Sessions Started or Ended	0	PASS	Detailed Report	
2.2.C	Resources	System Security Audit Journal Exists	0	PASS	Detailed Report	
5.1	Resources	Integrated File System Security	1	FAIL	Detailed Report	
2.2.C	Configuration	System, User, and Object Auditing Control Configuration	0	PASS	Detailed Report	
10.2	Configuration	Attention Events are Audited	0	PASS	Detailed Report	
10.2	Configuration	Authorization Failures are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Object Creations are Audited	0	PASS	Detailed Report	
10.2	Configuration	All Deletions of External Objects on the System are Audited	0	PASS	Detailed Report	
10.2	Configuration	Actions that Affect a Job are Audited	0	PASS	Detailed Report	
10.2	Configuration	Networking and Communications Functions are Audited	0	PASS	Detailed Report	
10.2	Configuration	Object Management Tasks are Audited	0	PASS	Detailed Report	

8.2. 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.

1) Administrative Safeguards – policies and procedures designed to clearly show how an organization will comply with the act

2) Physical Safeguards – controlling physical access to protect against inappropriate access to protected data

3) 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
164.308	Profiles	A logon or logoff operation on the network	0	PASS	Detailed Report
164.308	Profiles	All authority failures	1	FAIL	Detailed Report
164.308	Profiles	Enabled IBM Profiles	55	FAIL	Detailed Report
164.308	Profiles	Powerful user profiles	11	FAIL	Detailed Report

8.3. 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*

8.4. 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.

8.5. 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
6808	Resources	Public Authority in Library QGPL Not Exclude	127	FAIL	Detailed Report
6802	Profiles	Password expiration interval	0	PASS	Detailed Report
6802	Profiles	Password expiration warning	1	FAIL	Detailed

8.6. Standards Australia

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.

8.7. ISO 27001

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

9. Report Customization

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

Features available through the TGAudit reporting engine include:

- Defining the desired columns for a report
- Defining selection criteria using operation codes similar to SQL
- Nesting of selection criteria up to 5 levels
- Field order selection
- Defining report defaults to optimize report run efficiency
    - This feature essentially allows you to filter the data source collection the report is based on, so the report run is as targeted as possible.
- Specially defined date functions (allow you to do date comparisons using number of days)
- Defining report categories
- Copying existing report definitions

9.1. Creating Reports

To create a custom report, from the TGAudit Main Menu (TGMENU), select option 30 to “Work with Reports" or, from an IBM i command line, enter TGWRKRPT.

```
                                Work with Reports


 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID    Report Name
 =  Authority_List  Authorization List Details
 _  Authority_List  Authorization Lists with Public Access
 _  Controller_Atta Controllers and Attached Devices
 _  Controller_Desc Controller Description Details
 _  Device_Descript Device Descriptions - *APPC
 _  Device_Descript Device Description Details
 _  Exit_Points     Integrated File System Exits installed
 _  Exit_Points     Sockets-related Exit Points Not Secured
 _  Exit_Points     Unsecured Remote Server Exit Points
 _  IFS_Attributes  ASCII Files Stored in the IFS
 _  IFS_Attributes  Files Checked Out Status
 _  IFS_Attributes  IFS Directory Information
 _  IFS_Attributes  File Usage Information
 _  IFS_Attributes  Largest Files Report > 100Mb
 _  IFS_Attributes  Attributes for /QSYS.LIB                                +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

Step 1 - Define Report Name and Collector

From the “Work with Reports” screen, press F6 to add a new report:

```
                                Work with Reports


 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID    Report Name
 _  Authority_List  Authorization List Details
 _  Authority_List  Authorization Lists with Public Access
 _  Controller_Atta Controllers and Attached Devices
 _  Controller_Desc Controller Description Details
 _  Device_Descript Device Descriptions - *APPC
 _  Device_Descript Device Description Details
 _  Exit_Points     Integrated File System Exits installed
 _  Exit_Points     Sockets-related Exit Points Not Secured
 _  Exit_Points     Unsecured Remote Server Exit Points
 _  IFS_Attributes  ASCII Files Stored in the IFS
 _  IFS_Attributes  Files Checked Out Status
 _  IFS_Attributes  IFS Directory Information
 _  IFS_Attributes  File Usage Information
 _  IFS_Attributes  Largest Files Report > 100Mb
 _  IFS_Attributes  Attributes for /QSYS.LIB                              +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

From the list of Data Collectors that appears, select the most relevant for the desired report:

```
CMN80200R-02                    Report Definition

     Sel
     (X) Collector Name
      _  Authority List Information
      _  Controller Attached Device Information
      _  Controller Description Information
      _  Data Area Changes
      _  Database Changes
      _  Device Description APPC Information
      _  Device Description Information
      _  Exit Point Information
      _  Field Level Authorities
      _  IFS Object Attributes
      _  IFS Authorities
      _  IFS Extended Journaling Information
      _  IFS stat() Status Information
      _  IFS Status Information
                                                              More...
          ENTER=Select        F12=Cancel

 F3
```

Enter a Report ID and Report Name, as well as a Category. The Report ID should not contain spaces. The Report Name should describe the data that will appear in the report. The main categories of reports within the product are: Configuration, Resources, Profiles, and Network. You may also create customized categories by just typing a new category name.

If the new report being created is applicable to any of the regulations shown on the screen, enter the regulation clause number. This will add the report you defined to the applicable regulation Report Card and the next time you run the regulation Report Card, this new report will be included.

```
CMN80200R-02                    Report Definition

            Collector ID:  User_Profiles

            Report ID...:  AllUsers

            Report Name.:  All User Profiles

            Category....:  Profiles

            Regulatory Compliance
            PCI..........: __________
            GLBA.........: __________
            FISMA........: __________
            HIPAA........: __________
            SOX..........: __________
            Std Australia: __________
            ISO 27001....: __________

F3=Exit   F4=Select Collector   F12=Cancel    Enter=Update
```

Step 2 - Select Report Columns

To define the columns to appear on the report, select option 8 for the applicable report and press Enter:

```
                              Work with Reports

 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID    Report Name
 _  System_Values   Server Security Data is Retained
 _  System_Values   Remote Power On and IPL
 _  System_Values   Remote Sign-on Control
 _  System_Values   Remote Service Attribute
 _  System_Values   Strong System Security Level
 _  System_Values   Time adjustment software Installed
 _  System_Values   Restricted use of Use Adopted Authority
 _  System_Values   Verify Object on Restore
 _  System_Values   SSL Cipher Control and Specification List
 _  System_Values   Security System Values
 _  TCPIPv4_Stack_A TCPIPv4 Stack Attributes
 _  TCPIPv6_Stack_A TCPIPv6 Stack Attributes
 8  User_Profiles   All User Profiles
 _  User_Profiles   Enabled IBM Profiles
 _  User_Profiles   User Profiles Not Used in 90 Days                  +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

By default, all field columns from the data source collector are selected when creating a new report.

```
 CMN80200R-03                    Report Field Selection

                                     Collector ID    : User_Profiles
  Select option, press ENTER         Report ID       : AllUsers
      4=Delete                       Report Name     : All User Profiles


  *** All fields related to the appliable collector are selected. ***

Opt Seq  Name       Description
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____                                                                  +


 F3=Exit  F4=Select Fields  F12=Cancel
```

To customize the columns that appear on the report, press F4 to select the fields:

```
 CMN80200R-03                    Report Field Selection

                                     Collector ID    : User_Profiles
  Select option, press ENTER         Report ID       : AllUsers
      4=Delete                       Report Name     : All User Profiles


  *** All fields related to the appliable collector are selected. ***

Opt Seq  Name       Description
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____
 _  ____                                                                  +


 F3=Exit  F4=Select Fields  F12=Cancel
```

Select the desired columns/field(s) for the report on the field selection window:

```
CMN80200R-03                    Report Field Selection

  Select option                 Sel Field      Collector ID  User_Profiles
      4=Delete                  (X) Name        Description
                                 _  UPDCEN      Display century: 0-19xx, 1-20xx
                                 _  UPDDAT      Display date: YYMMDD
  *** All field                  _  UPDTIM      Display time
                                 _  UPSYST      System
Opt Seq  Name                    X  UPUPRF      User Profile Name
 _  ____                         X  UPUSCL      User class
 _  ____                         X  UPDSIN      Display sign-on information
 _  ____                         _  UPPWCC      Password change century: 0-19xx, 1-20xx
 _  ____                         X  UPPWCD      Password change date: YYMMDD
 _  ____                         X  UPPWCT      Password change time
 _  ____                         X  UPPWEI      Password expiration interval
 _  ____                         X  UPPWEX      Password set expired by command
 _  ____                         X  UPPWON      Password is *NONE: *YES or *NO
 _  ____                            UPPSOC      Previous sign-on century: 0-19xx, 1-20xx
 _  ____                                                                      More...
                                        ENTER=Select        F12=Cancel

 F3=Exit  F4=Se
```

Column order can be adjusted by changing the sequence numbers in the “Seq” column:

```
CMN80200R-03                    Report Field Selection

                                   Collector ID    : User_Profiles
  Select option, press ENTER       Report ID       : AllUsers
      4=Delete                     Report Name     : All User Profiles



Opt Seq  Name       Description
 _   10  UPUPRF     User Profile Name
 _   20  UPUSCL     User class
 _   30  UPDSIN     Display sign-on information
 _   40  UPPWCD     Password change date: YYMMDD
 _   50  UPPWCT     Password change time
 _   60  UPPWEI     Password expiration interval
 _   70  UPPWEX     Password set expired by command
 _   80  UPPWON     Password is *NONE: *YES or *NO
 _  ____
 _  ____                                                                        +


 F3=Exit  F4=Select Fields  F12=Cancel
```

Press Enter to confirm field selections, then press F12 to return to the “Work with Reports” screen.

Step 3 - Define Filter Details

To customize specific search criteria for a report, create a report filter by selecting option 9 next to the applicable report on the “Work with Reports” screen:

```
                                Work with Reports


 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID     Report Name
 _  System_Values    Server Security Data is Retained
 _  System_Values    Remote Power On and IPL
 _  System_Values    Remote Sign-on Control
 _  System_Values    Remote Service Attribute
 _  System_Values    Strong System Security Level
 _  System_Values    Time adjustment software Installed
 _  System_Values    Restricted use of Use Adopted Authority
 _  System_Values    Verify Object on Restore
 _  System_Values    SSL Cipher Control and Specification List
 _  System_Values    Security System Values
 _  TCPIPv4_Stack_A  TCPIPv4 Stack Attributes
 _  TCPIPv6_Stack_A  TCPIPv6 Stack Attributes
 9  User_Profiles    All User Profiles
 _  User_Profiles    Enabled IBM Profiles
 _  User_Profiles    User Profiles Not Used in 90 Days                    +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

Report filters can be created using any fields available in the collector data source on which the report is built. The fields in the report filter do not necessarily have to be included in the report.

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

```
Operation Codes
 >     Greater Than
 <     Less Than
 >=    Greater or Equal To
 <=    Less Than or Equal To
 =     Equal To
 <>    Not Equal To
Like   Like
Notl   Not Like
YMD>   Greater Than XX Days
YMD<   Less Than XX Days
```

To select the fields to be used in the report filter, press F4, select one or multiple fields, then press Enter. The selected fields will appear in the “Field Name” column. Edit the search criteria by inputting operators and comparison values. Up to five levels of nesting can be used. 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.

```
CMN80200R-03                    Report Filter Details

                                   Collector ID    : User_Profiles
 Select option, press ENTER        Report ID       : Enabled_IBM_Profiles
     4=Delete                      Report Name     : Enabled IBM Profiles



    AND/ Nest  Field     Operator                                          Nest
Opt OR   Str   Name       Value  Value (quotes are not needed)             End
 _  ____ _____ UPUPRF     LIKE   Q%                                        _____
 _  AND  _____ UPSTAT     =      *ENABLED                                  _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ _____
 _  ____ _____            ____   ________________________________________ __ +


F3=Exit  F4=Select Fields  F9=Insert Line  F10=Display Op Codes  F12=Cancel
```

Step 4 - Define Report Defaults

Customizing the report defaults for the data source collection of a report enables you to maximize how efficiently the report will run. Report defaults provide options specific to the data source collector the report is based on, 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 have the ability to specify particular date ranges so that any report filters are only run across a subset amount of data instead of the entire range of what may be available.

Report Defaults are processed before any report run-time options, except in cases where the report run-time option specifies "Y" to override report defaults.

```
                                Work with Reports

 2=Edit 3=Copy 4=Delete 6=Defaults 7=Run 8=Field List 9=Filter

Opt Collector ID     Report Name
 _  Journal_OM       Object Management Changes
 _  Journal_OR       Objects Restored
 _  Journal_OR       Newly Restored Objects
 _  Journal_OW       Object Ownership Changes
 _  Journal_O1       Single Optical Object Accesses
 _  Journal_O2       Dual Optical Object Accesses
 _  Journal_O3       Optical Volume Accesses
 _  Journal_PA       Program Changes to Adopt Owner Authority
 _  Journal_PF       PTF Operations
 _  Journal_PG       Primary Group Changes
 _  Journal_PO       Printer Output Changes
 _  Journal_PS       Swap Profile Events
 _  Journal_PU       PTF Object Changes
 _  Journal_PW       Invalid Sign-on Attempts
 _  Journal_RA       Authority Changes to Restored Objects                +

 F1=Help   F3=Exit   F6=Add Report   F12=Cancel
```

```
                                Report Defaults



             Collector ID:   Journal_OR
             Report ID...:   Rst_Objs
             Report Name.:   Newly Restored Objects

             User Name...:   *ALL       (Name, generic*, *ALL)


             From Date...:   *LWS       (Date, *LMS,*LME,*CMS,*LWS,*LDS,*CUR)
             From Time ..:   _______    (Time (hhmmss))
             To Date.....:   *CUR       (Date, *LMS,*LME,*CMS,*LWS,*LDS,*CUR)
             To Time.....:   ________   (Time (hhmmss))



 F3=Exit   F12=Cancel  Enter=Update
```

User Name - Enter user name, generic user name, or *ALL

From Date - Enter specific date or one of the special dates below

From time - Enter specific time

To Date - Enter specific date or you may enter one of the special dates below

To time - Enter specific time

Special Date Values	
*CUR	Current day
*CMS	Current month start
*LMS	Last month start
*LME	Last month start
*LYS	Last year start
*LYE	Last year end
*LWS	Last week start (current date minus 7 days)
*LDS	Last day start

9.2. Modifying Reports

Report definitions, defaults, fields/columns, and report filters can be modified through the “Work with Reports” screen. Note that built-in reports cannot be edited. Please refer to “Creating Reports” for details on options 6, 8, and 9.

Option 2 allows you to modify the Report Name, Category, and regulation details in the “Report Definition”. The Report ID cannot be edited after the Report is created.

Option 6 allows you to update Report Defaults to customize the data source collection of the report.

Option 8 allows you to modify the column selection of the report. The order the columns are displayed can also be modified.

Option 9 allows you to edit the search criteria of the report.

9.3. Copying Reports

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. Use option 3 from the “Work with Reports” screen to copy an existing report. Enter a new unique Report ID and continue customization as desired. Please refer to “Creating Reports” for details.

9.4. Deleting Reports

From the “Work with Reports” screen, use option 4 to delete an existing report. Note that built-in reports cannot be deleted.

10. Report Card Customization

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. 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 TGAudit which 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” screen, select option 31 from the TGAudit Main Menu or type TGWRKCARD from a command line and press Enter.

```
                              Work with Report Cards

 2=Change   3=Copy   4=Delete   7=Run   9=Select Reports

Opt Report Card ID       Report Card                              Category
 _  FISMA                Federal Information Security Management Regulations
 _  GLBA                 Gramm-Leach-Bliley Act                   Regulations
 _  HIPAA                Health Insurance Portability and Accoun Regulations
 _  IFS_Reports          Integrated File System Reports           IFSReports
 _  ISO_27001            Information security management system  Regulations
 _  PCI                  PCI DSS 3.1                              Regulations
 _  PCI_20               PCI DSS 2.0                              Regulations
 _  Security_Assessment  TGFree Security Assessment               Analysis
 _  STDAUS               Standard Australia                       Regulations





 F1=Help   F3=Exit   F6=Add Report Card    F12=Cancel
```

10.1. Creating Report Cards

To create a custom Report Card, from the TGAudit Main Menu (TGMENU), select option "31. Work with Report Cards" or, from an IBM i command line, enter TGWRKCARD and follow the steps below.

Step 1 - Define Report Card Name

From the “Work with Report Cards” screen, press F6 to add a new Report Card:

```
                              Work with Report Cards

 2=Change   3=Copy   4=Delete   7=Run   9=Select Reports

Opt Report Card ID       Report Card                              Category
 _  FISMA                Federal Information Security Management Regulations
 _  GLBA                 Gramm-Leach-Bliley Act                   Regulations
 _  HIPAA                Health Insurance Portability and Accoun Regulations
 _  IFS_Reports          Integrated File System Reports           IFSReports
 _  ISO_27001            Information security management system  Regulations
 _  PCI                  PCI DSS 3.1                              Regulations
 _  PCI_20               PCI DSS 2.0                              Regulations
 _  Security_Assessment  TGFree Security Assessment               Analysis
 _  STDAUS               Standard Australia                       Regulations

 F1=Help   F3=Exit   F6=Add Report Card   F12=Cancel
```

Enter a Report Card ID, a Report Card Name, and a Category. If you need the capability of entering references for compliance regulation clauses in your Report Card, enter a “Y” in the Regulation parameter. This can help you map reports to particular sections of a compliance regulation document or security policy. Otherwise, enter “N” and press Enter twice.

```
                              Report Card Definition


       Report Card ID....:  SOX

       Report Card Name..:  Sarbanes-Oxley
                            ____________________________
       Category..........:  Regulations

       Regulation........:  Y (Y/N)


 F3=Exit   F12=Cancel   Enter=Update
```

Step 2 - Define Report List

To choose the reports to be included in the Report Card, select option 9 from the “Work with Report Cards” screen:

```
                              Work with Report Cards


 2=Change   3=Copy   4=Delete   7=Run   9=Select Reports

Opt Report Card ID       Report Card                              Category
 _  FISMA                Federal Information Security Management Regulations
 _  GLBA                 Gramm-Leach-Bliley Act                   Regulations
 _  HIPAA                Health Insurance Portability and Accoun Regulations
 _  IFS_Reports          Integrated File System Reports           IFSReports
 _  ISO_27001            Information security management system  Regulations
 _  PCI                  PCI DSS 3.1                              Regulations
 _  PCI_20               PCI DSS 2.0                              Regulations
 _  Security_Assessment  TGFree Security Assessment               Analysis
 9  SOX                  Sarbanes-Oxley                           Regulations
 _  STDAUS               Standard Australia                       Regulations




 F1=Help   F3=Exit   F6=Add Report Card    F12=Cancel
```

```
                                 Select Reports


  Select option, press ENTER     Report Card ID :  SOX
      4=Delete                   Report Card    :  Sarbanes-Oxley


                                    --PASS CRITERIA--            ---LAST RUN---
     Report                          Comp  Number of  Regulation Last Run  Pass/
 Opt Name                            Cond  Rows       Clause     Rows      Fail
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0
  _                                  ____  ________0  __________        0    +


 F3=Exit  F4=Select Report  F10=Display Op Codes  F12=Cancel
```

From the “Select Reports” screen, press F4 and select the desired reports for the Report Card:

```
                                   Select Reports


 Select option, press ENTER      Report Card ID :  SOX
     4=Delete                    Report Card    :  Sarbanes-Oxley


                                    --PASS CRITERIA--              ---LAST RUN---
    Report                           Comp  Number of  Regulation  Last Run  Pass/
Opt Name                             Cond  Rows       Clause      Rows      Fail
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0
 _                                   ____  ________0  __________         0    +

F3=Exit  F4=Select Report  F10=Display Op Codes  F12=Cancel
```

```
                                   Select Reports

 Select      Sel
     4=      (X) Report Name
              X  Object Auditing Attribute Changes
              X  Authority Failures
              _  Programs that Adopt Authority were Executed
    Rep       _  EIM Attribute Changes                                          /
Opt Nam       _  Row and Column Access Control
 _            X  Authorization List or Object Authority Changes
 _            _  Commands Executed
 _            _  Create Operations
 _            X  User Profile Changes
 _            _  Change Request Descriptor Changes
 _            _  Cluster Operations
 _            _  Connection Verifications
 _            _  Cryptographic Configuration Changes
 _            _  LDAP Operations
 _                                                                  More...
                 ENTER=Select        F12=Return

F3=Exit
```

Step 3 - Define Pass Criteria

After all reports are selected, define what is acceptable for report results and cause the report to “pass” on the Report Card. This is called “pass criteria.” A comparison condition and the number of rows returned in the report make up the pass criteria.

The values valid for the comparison condition can be displayed using F10 to Display Op Codes.

> Greater Than
< Less Than
>= Greater Than or Equal To
<= Less Than or Equal To
= Equal To
<> Not Equal To

Using these operation codes, you can create comparison conditions that define passing criteria for a report. 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. To set the report to pass only when there are no user profile changes on the system, define the pass criteria so the report passes only when there are no user profile changes (ie: less than one). When the Report Card is run with this definition, the report will display a failing result if there are one or more user profile changes and allow you to click on the fail grade to see the detailed report showing changes made to user profiles.

```
                                  --PASS CRITERIA--
    Report                         Comp  Number of
Opt Name                           Cond  Rows
 _  Sockets-related Exit Points No  <     _________1
 _  Unsecured Remote Server Exit P  <     _________1
 _  Object Auditing Attribute Chan  <     _________1
 _  Authority Failures              <     _________1
 _  Authorization List or Object A  <     _________1
 _  User Profile Changes            <     _________1
```

Step 4 – Define Regulation Clauses

If the Report Card you are creating is being created to map to a particular compliance regulation or security policy document, you can additionally label reports to corresponding sections of the document by adding descriptive text for section identifiers in the Regulation Clause column.

For example:

```
 Select option, press ENTER     Report Card ID : SOX
     4=Delete                   Report Card    : Sarbanes-Oxley


                                  --PASS CRITERIA--
    Report                         Comp  Number of  Regulation
Opt Name                           Cond  Rows       Clause
 _  Sockets-related Exit Points No  <     _________1  LA-5
 _  Unsecured Remote Server Exit P  <     _________1  LA-5
 _  Object Auditing Attribute Chan  <     _________1  ASIM-14
 _  Authority Failures              <     _________1  LA-1
 _  Authorization List or Object A  <     _________1  ASIM-14
 _  User Profile Changes            <     _________1  LA-1
 _  Changes to Service Tools Profi  <     _________1  LA-1
 _  Intrusion Monitor Events        <     _________1  OP-8
 _  Network Attribute Changes       <     _________1  ASIM-14
 _  Program Changes to Adopt Owner  <     _________1  ASIM-14
```

10.2. Modifying Report Cards

Existing Report Cards can be edited by using options 2 and 9 on the “Work with Report Cards” screen. Note that built-in Report Cards cannot be edited.

Option 2 allows you to modify the Report Card Name and Category in the “Report Card Definition”. The Report Card ID cannot be edited after the Report Card is created.

Option 9 allows you to add or remove reports from the Report Card, change pass criteria, and edit regulation clause text in the “Select Reports” screen. If the Report Card has been previously run, the “Select Reports” screen also displays the number of rows returned for each report the last time it was run and whether or not that number of rows gave a pass or fail grade.

10.3. Deleting Report Cards

Report Cards can be deleted in the “Work with Report Cards” screen by selecting option 4 next to the desired Report Card and pressing Enter. Note that built-in Report Cards cannot be deleted.

11. Product Management

To manage TGAudit options, use F17=TG Management from the TGAudit Main Menu (TGMENU).

```
TGMCONFIG                          Product Management

Select one of the following:

     1. Work with TG Product Users
     2. Licensing Status

    21. Reporting Configuration
    22. HTML Reporting Attributes

                                                                    Bottom
Selection or command
===>
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
```

Option 1 – Work with TG Product Users

This option allows you to control who can access TGAudit by editing the TGAUTL authorization list. The authority defined in this authorization list defines the users' authority to TGAudit functionality.

To grant a user authority to use TGAudit, press F6 and enter the user profile and *ALL object authority. To remove a user's authority to TGAudit, delete the object authority for the user and press Enter.

```
                              Edit Authorization List

Object . . . . . . . :   TGAUTL          Owner  . . . . . . . :   TGOWNER
  Library  . . . . . :     QSYS          Primary group  . . . :   *NONE

Type changes to current authorities, press Enter.

             Object    List
User        Authority  Mgt
*PUBLIC     *EXCLUDE    _
TGOWNER     *ALL        X
QSECOFR     *ALL        _

                                                                    Bottom
F3=Exit   F5=Refresh   F6=Add new users
F11=Display detail object authorities   F12=Cancel   F24=More keys
```

Option 2 – Licensing Status

This option allows you to view current TGAudit software licensing information and add new license keys.

```
                          Work with Licensing Status


 System Information :
    Serial Number  . . . . . . . . . . [redacted]
    Processor Group  . . . . . . . . . P05
    OS Version . . . . . . . . . . . . V7R1M0


 License Information :
    Product Version  . . . . . . . . . 1.3.00016
    Expiration Date  . . . . . . . . . [redacted]      (YY/MM/DD)

    TGTravel Allowed . . . . . . . . . N            (Y=Yes N=No)
    TGAudit Allowed  . . . . . . . . . Y            (Y=Yes N=No)





 F1=Help   F3=Exit   F6=Add Key
```

Option 21 – Reporting Configuration

This option allows you to edit the TGAudit configuration file for advanced report output configuration.

```
 Edit File: /etc/TrinityGuard.cfg
 Record : _____1   of       7 by  10                    Column : ___1     59 by 126
 Control : ____________________________________________________________________

CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....+..
     ************Beginning of data**************
___ home=/TrinityGuard
___ headings=2
___ label=*COLHDG
___ encode=*NO
___ schema=*YES
___ fielddelimiter=,
___ outputCCSID=819
     ************End of Data********************


 F2=Save  F3=Save/Exit   F12=Exit   F15=Services   F16=Repeat find   F17=Repeat change   F19=Left   F20=Right
```

Option 22 – HTML Reporting Attributes

This option allows you to edit advanced style configuration for all TGAudit HTML report output.

```
WORK WITH DATA IN A FILE                          Mode . . . . :   CHANGE
Format . . . . :   TGCFGHTML                      File . . . . :   TGCFGHTML

*RECNBR:                    1
Style Sheet Name:  _
Heading Font:      Helvetica,Arial,sans-serif
Heading Color:     Black
Sub Heading Font:  Helvetica,Arial,sans-serif
Sub Heading Color: Blue
Border Color:      Black
Border Type:       1
Table Font:        Helvetica,Arial,sans-serif

F3=Exit                 F5=Refresh              F6=Select format
F9=Insert               F10=Entry               F11=Change
```

12. Troubleshooting Reference

12.1. Uninstall steps

To uninstall TGAudit, execute the following commands at an IBM i command line:

1. TGINSTALL/TGINSTALL PROD(*TGAUDIT) INSTYPE(*REMOVE)
2. DLTLIB LIB(TGINSTALL)
3. DLTUSRPRF USRPRF(TGOWNER)
4. DLTAUTL AUTL(TGAUTL)

12.2. CPF4169 While Accessing Menu Options

If you encounter a run-time error with message ID CPF4169 while accessing any of the TGAudit menu options, it is likely because the emulator you are using has a display size of 24x80. Please re-try accessing the product using a workstation emulation display size of 27x132. TGAudit does not support workstations displays of 24x80.

APPENDIX A

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 a IFS file with stat()	IFS_Stat_Data
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
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
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
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
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	Basic Information including principal and additional libraries about a software product	Product_Info_Libs
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