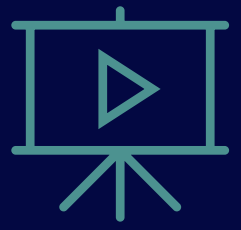
Top 5 Tasks for IBM i Admins

FRESCHE SOLUTIONS

Housekeeping



Get the slides & session recording via email

Ask questions

Share your thoughts

FRESCHE SOLUTIONS

Carol Woodbury
CTO, DXR Security

Alan Hamm
Senior Security Engineer, Fresche

Agenda

- Introduction
- Top 5 Tasks for IBM i Admins
- Ways to Automate These Tasks
  - System Values
  - User Profiles
  - Protecting Data
  - Actions to Review from the Audit Journal
  - Evidence – Supporting Documentation – Reporting
- Fresche's Solutions
- Next Steps

Top Five
IBM i Security Admin Tasks You May Be Missing

Carol Woodbury, CISSP, CRISC

IBM CHAMPION

carol@dxrsecurity.com

DXR SECURITY

© DXRSecurity, All Rights Reserved.

Why are We Talking About This?

When security is not administered, it typically becomes ‘undone.’

DXR SECURITY

System Values

- Ensure they meet security best practices:
  - IBM i Security Reference
  - IBM i Security Administration and Compliance, Third edition
  - Risk Assessment output
- Where they don't, evaluate the risk:
  - Of changing
  - Of not changing
- Key system values:
  - QSECURITY
  - QPWD*
  - QMAXSIGN
  - QAUD*
  - QCRTAUT
  - QSSL*

DXR SECURITY

User Profiles

DXR SECURITY

Reviewing User Profile Capabilities

- Group profile assignments
- Special authorities
- Limited capability setting

DXR SECURITY

Working with User Profiles

Traditional interfaces:

- WRKUSRPRF cw* or *ALL
- CRT/CHG/DLTUSRPRF
- PRTUSRPRF
- DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(your_lib/your_file)

Modern interfaces:

- Navigator for i
- IBM Service: QSYS2.user_info

DXR SECURITY

Service Account Setting Recommendations

- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible. Do not default to *ALLOBJ!
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)
  - TEXT('Something informative')
  - PASSWORD -> Not a default!
  - PWDEXPITV -> Recommend the pwd be changed periodically

⇨ Add rules in exit point products to stop these profiles from being used for other purposes.

DXR SECURITY

Groups / Ownership Account Setting Recommendations

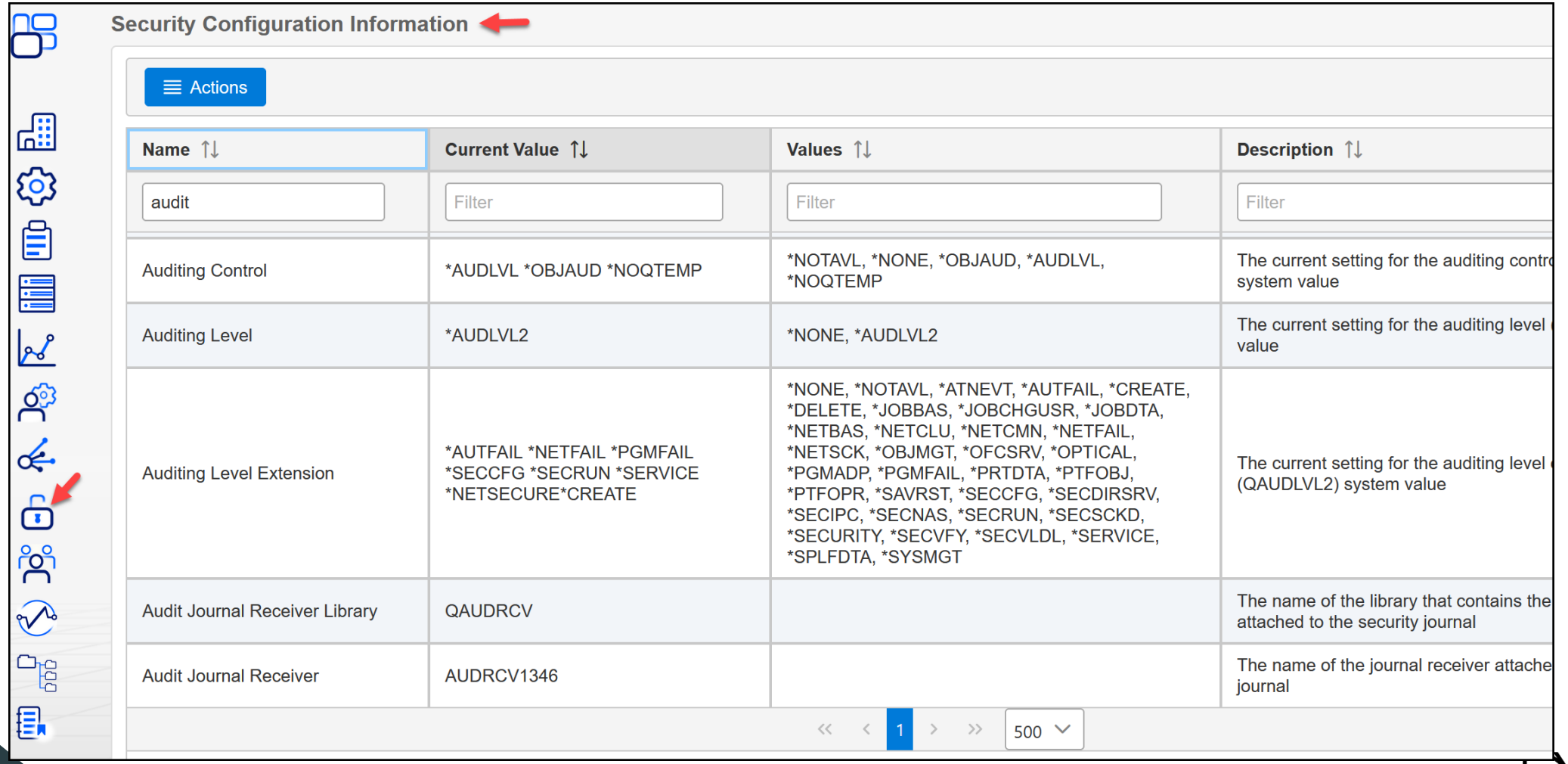
- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible
  - PASSWORD(*NONE)
  - PWDEXPITV(*SYSVAL)
  - STATUS(*DISABLED)
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)

DXR SECURITY

Protecting Data

DXR SECURITY

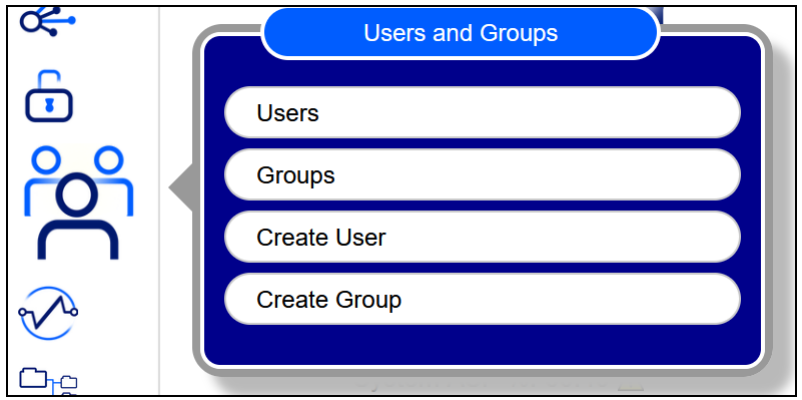
Working with System Values



http://your_system_name:2002/Navigator/login

DXR SECURITY

Users (or Groups) – Navigator for i



IBM Navigator for i

Search common1 cwoodbury

Users

Actions

Name	Profile Status	Special Authorities	Description	Group	Supplemental Groups	Profile Type	NetServer Disabled
c	Filter	*ALLOBJ	Filter	Filter	Filter	Filter	Filter
CWOODBURY2	*ENABLED	*ALLOBJ		*NONE		User	NO
CGUARINO	*DISABLED	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG	Charles Guarino - Demo Presenter	*NONE		User	NO
CGUARINO1	*DISABLED	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG	Charles Guarino - Demo Presenter	*NONE		User	NO

Profiles with a Default Password

```
38  --  Find user profiles with default passwords (password same as the user profile name)
39  --
40  select USER_NAME, STATUS, PASSWORD_EXPIRATION_INTERVAL, SPECIAL_AUTHORITIES, GROUP_PROFILE_NAME,
41         SUPPLEMENTAL_GROUP_LIST, LAST_USED_TIMESTAMP, CREATION_TIMESTAMP, USER_CREATOR,
42         TEXT_DESCRIPTION
43    from qsys2.user_info
44    where USER_DEFAULT_PASSWORD = 'YES'
45    order by status;
```

Authorization Name USER_NAME	Status STATUS	Password Expiration Interval PASSWORD_EXPIRATION_INTERVAL	Special Authorities SPECIAL_AUTHORITIES	Group Profile Name GROUP_PROFILE_NAME	Supplemental Group List SUPPLEMENTAL_GROUP_LIST	Last Used Timestamp LAST_USED_TIMESTAM
AWONT	*DISABLED	0	*ALLOBJ	*NONE	-	-
BEDROCK02	*DISABLED	0	-	*NONE	-	-
BOAT	*DISABLED	0	-	*NONE	-	-
CHRISD	*DISABLED	0	*SECADM	*NONE	-	-
GENIEUSR01	*DISABLED	0	-	QPGMR	-	-
LABGIT	*DISABLED	0	-	*NONE	-	2020-09-16 00:00:00.000

Hints:

- Use this method to perform other analysis on user profile configuration. For example:
  - Profiles not limited *YES (not LMTCPB(*YES))
  - Profiles with a non-expiring password (PWDEXPITV(*NOMAX))
- Include (or remove) the other attributes selected so it makes sense for your reporting / analysis

DXR SECURITY

Listing Inactive Profiles with SQL

```
46 --
47 --  List User profiles that haven't been used in the last 3 months
48 --
49 SELECT user_name,
50       date(last_used_timestamp) as last_used,
51       timestamp(previous_signon, 0) as last_signon,
52       timestamp(creation_timestamp, 0) as create_time,
53       status,
54       text_description
55    FROM QSYS2.USER_INFO
56    WHERE (last_used_timestamp IS NULL
57           OR last_used_timestamp < CURRENT TIMESTAMP - 3 MONTHS)
58         AND (creation_timestamp < CURRENT TIMESTAMP - 3 MONTHS);
```

Authorization Name USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	Status STATUS	Text Description TEXT_DESCRIPTION
#GNOTEST	-	-	2022-01-03 09:07:31	*ENABLED	-
AAATIM4	-	-	2021-07-07 09:01:55	*ENABLED	asdfasdf
AARONC	2020-03-11	2020-03-11 09:03:36	2019-05-06 14:17:45	*ENABLED	-
AATIM	-	-	2018-08-27 07:41:53	*ENABLED	Setsrgee
AATIM3	-	-	2022-10-21 13:18:20	*ENABLED	Test users
ACADMN01	2020-09-15	2020-09-15 16:15:08	2019-05-02 17:05:31	*ENABLED	Admin user for authority collection

Make sure you're looking at the right date. Last used, NOT last sign-on!

DXR SECURITY

Security Must be More than Menu ‘Security’

Users downloading to an Excel spreadsheet

ODBC connections to Windows servers

FTP to banks, payroll processors, trading partners

Developers updating data

People using ACS features such as Run SQL Scripts

SSH

Administrators and Analysts with legitimate command line access

DXR SECURITY

Data May be in Either a Library or a Directory

- Data should be secured
  - For Integrity ->
    - *PUBLIC(*USE) for objects in a library
    - *PUBLIC DTAAUT(*RX) OBJAUT(*NONE) for objects in a directory
  - For Confidentiality ->
    - *PUBLIC(*EXCLUDE)
    - *PUBLIC DTAAUT(*EXCLUDE) OBJAUT(*NONE)
- Use Authority Collection to determine how much authority is required.

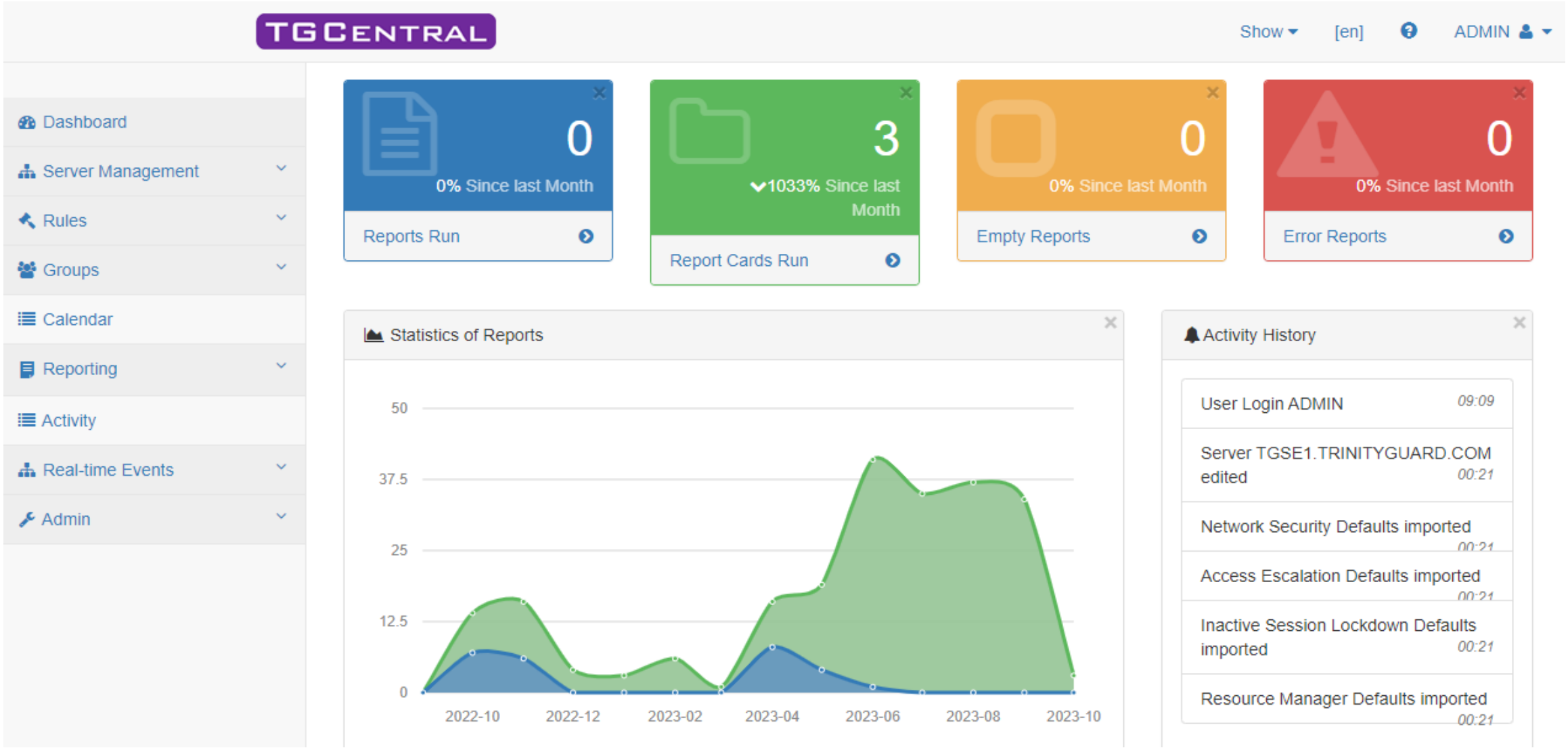
DXR SECURITY

To Review Object Authorities

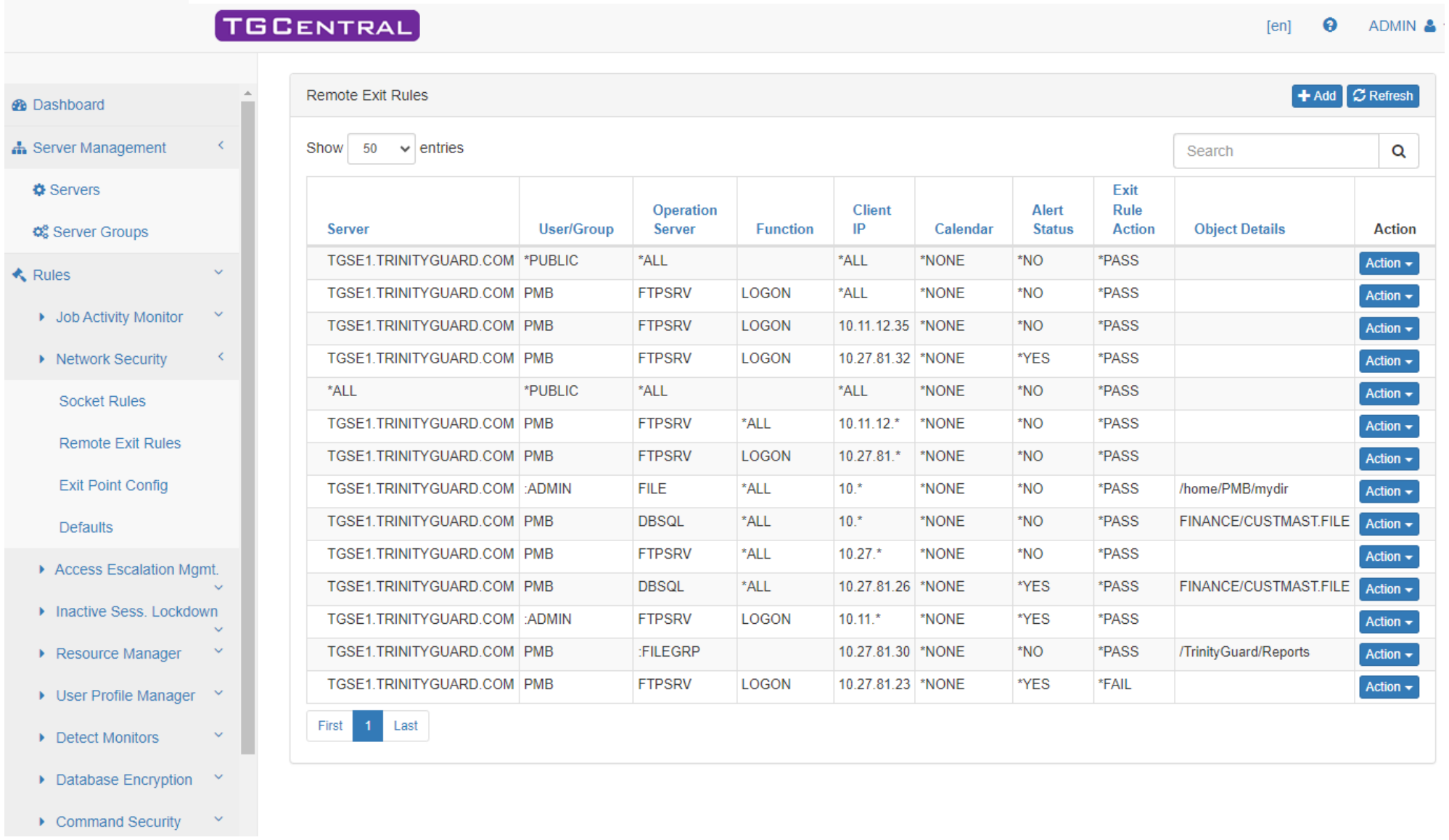
- QSYS2.object_privileges (same as the DSPOBJAUT command)
- QSYS2.ifs_object_privileges (same as the DSPAUT command)
- QSYS2.object_ownership (same as the WRKOBJOWN command or QSYLOBJA API)

DXR SECURITY

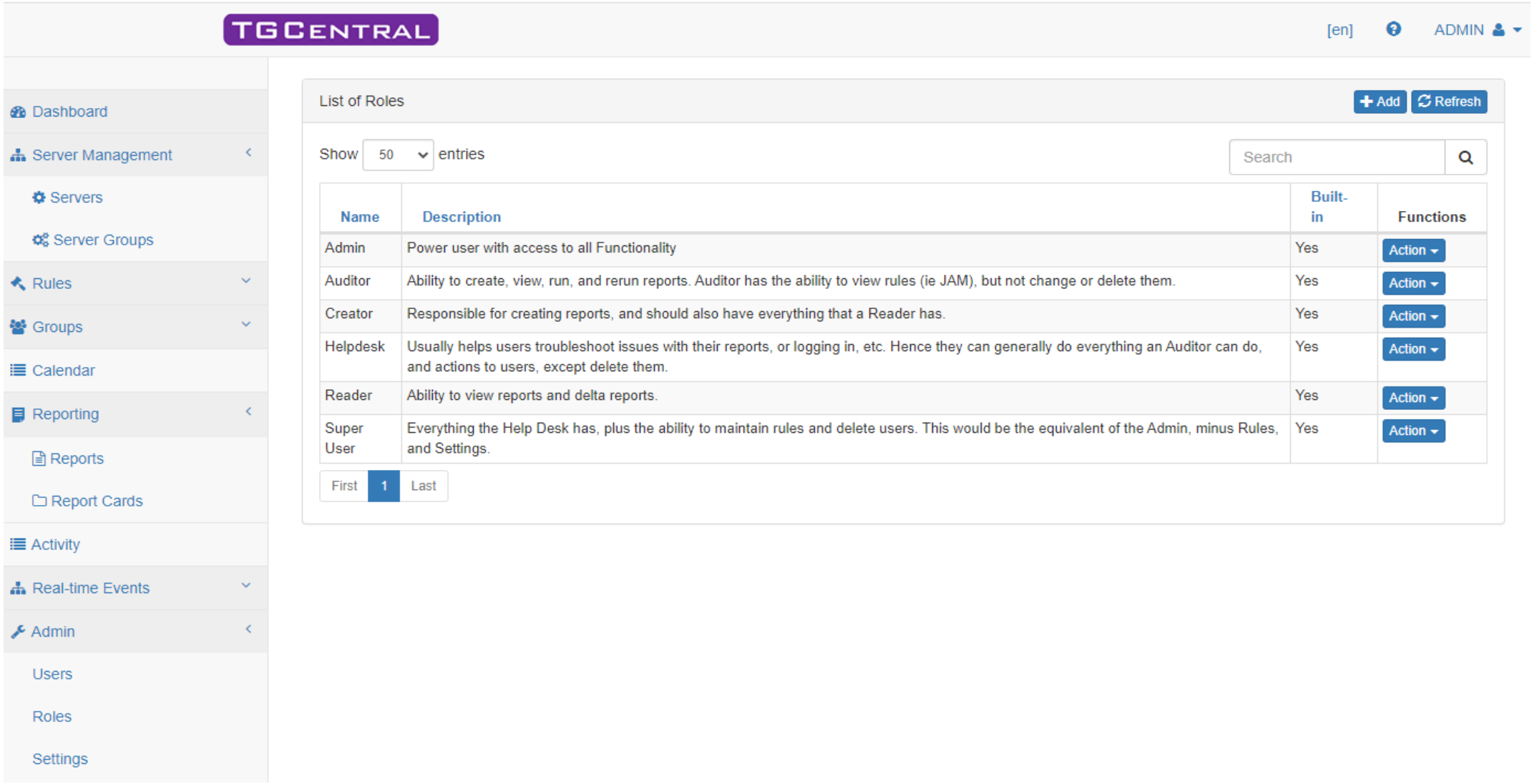
Fresche Security – The GUI



Fresche Security – The GUI



Fresche Security – The GUI



System Values

Security Configuration Information

Actions

Name	Current Value	Possible Values	Description
audit	Filter	Filter	Filter
Create Object Auditing	*NONE	*NONE, *USRPRF, *CHANGE, *ALL	The current setting for the create object auditing (QCRTOBJAUD) system value
Audit Journal Exists	YES	YES, NO	Whether the security journal QAUDJRN exists
Auditing Control	*AUDLVL *NOQTEMP *OBJAUD	*NOTAVL, *NONE, *OBJAUD, *AUDLVL, *NOQTEMP	The current setting for the auditing control (QAUDCTL) system value
Auditing Level	*AUDLVL2	*NONE, *AUDLVL2	The current setting for the auditing level (QAUDLVL) system value
Auditing Level Extension	*ATNEVT *AUTFAIL *CREATE *DELETE *JOBDTA *NETCMN *NETSCK *NETTELSVR*NETUDP *OBJMGT *OFCSRV *OPTICAL *PGMADP *PGMFAIL *PRTDTA *PTFOBJ *PTFOPR *SAVRST *SECURITY *SERVICE *SPLFDTA *SYSMGT	*NONE, *NOTAVL, *ATNEVT, *AUTFAIL, *CREATE, *DELETE, *JOBBAS, *JOBCHGUSR, *JOBDTA, *NETBAS, *NETCLU, *NETCMN, *NETFAIL, *NETSCK, *OBJMGT, *OFCSRV, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDTA, *PTFOBJ, *PTFOPR, *SAVRST, *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECURITY, *SECVFY, *SECVLDL, *SERVICE, *SPLFDTA, *SYSMGT	The current setting for the auditing level extension (QAUDLVL2) system value
Audit Journal Receiver Library	QGPL		The name of the library that contains the journal receiver attached to the security journal
Audit Journal Receiver	ZAUDJR1215		The name of the journal receiver attached to the security journal

« ‹ 1 › » 500

Filtered Rows: 7 | Total Rows: 46

System Values

System Values

Actions

Category	Description	System Values
Filter	Filter	Filter
Auditing	Changes auditing values	QAUDCTL, QAUDLVL, QAUDLVL2, QAUDENDACN, QAUDFRCLVL, QCRTOBJAUD
Date and Time	Changes date, time, and time zone information	QDATETIME, QCENTURY, QDAYOFWEEK, QDATE, QYEAR, QMONTH, QDAY, QLEAPADJ, QTIME, QHOUR, QMINUTE, QSECOND, QTIMADJ, QUTCOFFSET, QTIMZON
Devices	Changes device auto-configuration and recovery values	QAUTOCFG, QDEVNAMING, QAUTORMT, QAUTOVRT, QDEVRCYACN
International	Changes locale settings and format of numbers, currency, dates, and time	QDATFMT, QDATSEP, QTIMSEP, QDECFMT, QCURSYM, QLANGID, QCNTRYID, QKBDTYPE, QCCSID, QCHRID, QCHRIDCTL, QSRTSEQ, QIGC, QIGCCDEFNT, QIGCFNTSIZ, QLOCALE, QSETJOBATR
Jobs	Changes system level job limits and default job properties	QMAXJOB, QACTJOB, QTOTJOB, QADLACT, QADLTOT, QLOGOUTPUT, QJOBMSGQFL, QJOBMSGQMX, QINACTMSGQ, QDSCJOBITV, QMLTTHDACN, QSPLFACN, QJOBSPLA, QMAXSPLF, QENDJOBLMT, QALWJOBITP
Library Lists	Changes the default library lists	QSYSLIBL, QUSRLIBL
Messages and Service	Changes message, logging, and service information	QHSTLOGSIZ, QCFGMSGQ, QACGLVL, QSTSMSG, QPRBHLDITV, QSFWERRLOG, QSRVDMP, QRMTSRVATR
Password	Changes password expiration and validation	QPWDLVL, QPWDCHGBLK, QPWDVLDPGM, QPWDMINLEN, QPWDMAXLEN, QPWDRQDDGT, QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDRQDDIF, QPWDPOSDIF, QPWDRULES, QPWDEXPITV, QPWDEXPWRN
Performance	Changes performance values for processing, memory pools, communications, and database	QDYNPTYADJ, QDYNPTYSCD, QPFRADJ, QMAXACTLVL, QMCHPOOL, QBASPOOL, QBASACTLVL, QTSEPOOL, QCMNRCYLMT, QCMNARB, QPASTHRSVR, QQRYDEGREE, QQRYTIMLMT, QDBFSTCCOL, QLIBLCKLVL, QTHDRSCAFN, QTHDRSCADJ
Power Control	Changes power supply values	QUPSDLYTIM, QUPSMSGQ

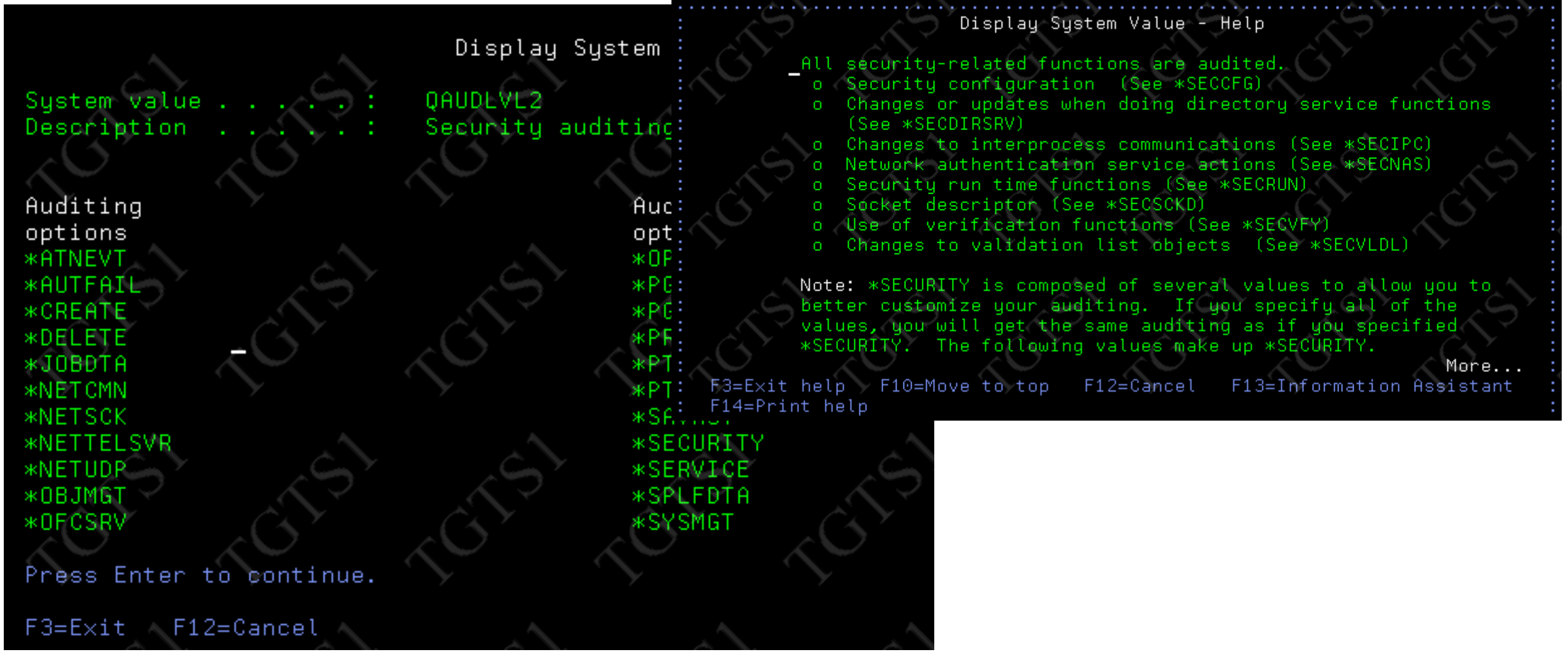
System Values

WRKSYSVAL QAUDLVL - Controls the level of action auditing on the

> *"If the QAUDLVL system value contains the value *AUDLVL2, then the values in the QAUDLVL2 system value will also be used. If the QAUDLVL system value does not contain the value *AUDLVL2, then the values in the QAUDLVL2 system value will be ignored. "*
> *– from QAUDLVL Extended help*

System Values

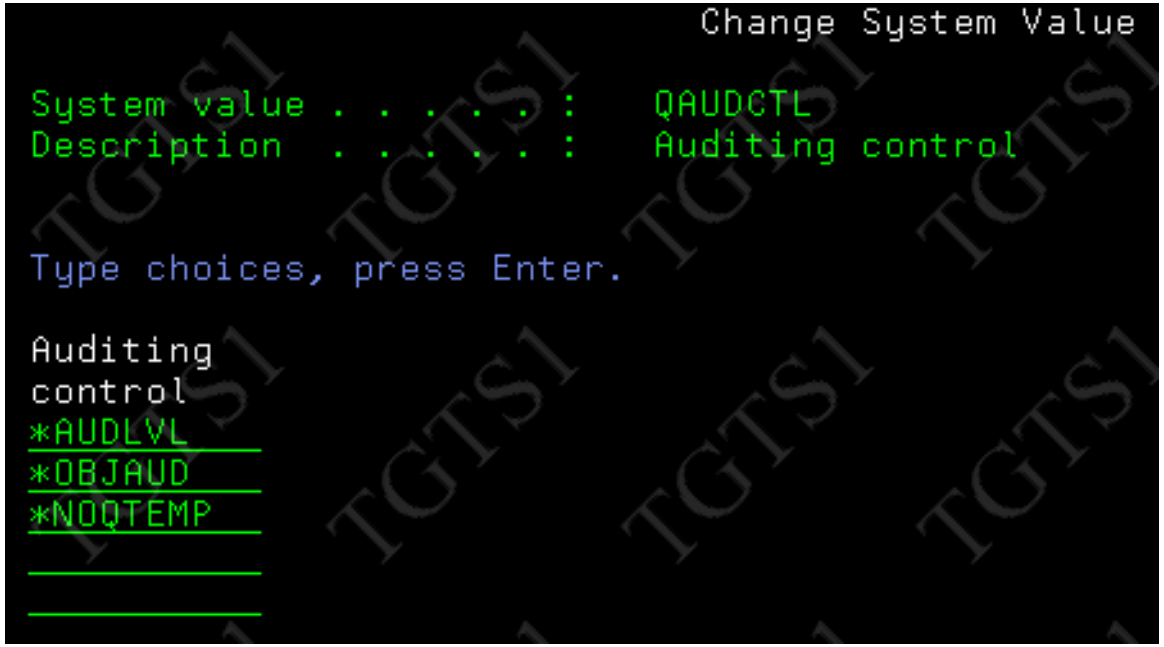
WRKSYSVAL QAUDLVL2



System Values

WRKSYSVAL QAUDCTL

*"A change to this system value takes effect immediately for all jobs running on the system. The shipped value is *NONE. "*
– from Audit control Extended help

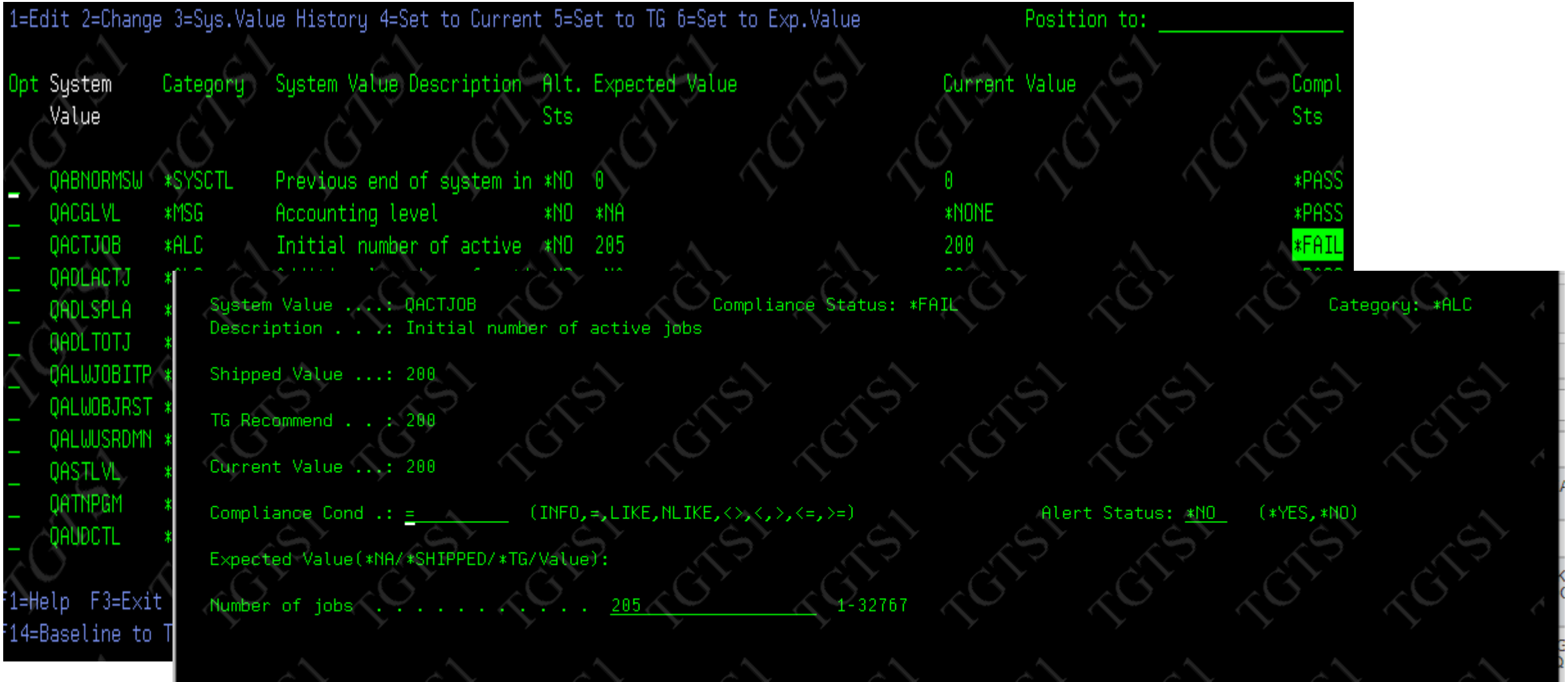


CHGSECAUD – What is this?

FRESCHE SOLUTIONS

System Values - Policy

Define System Values policy



System Values - Policy

Check compliance against System Values policy

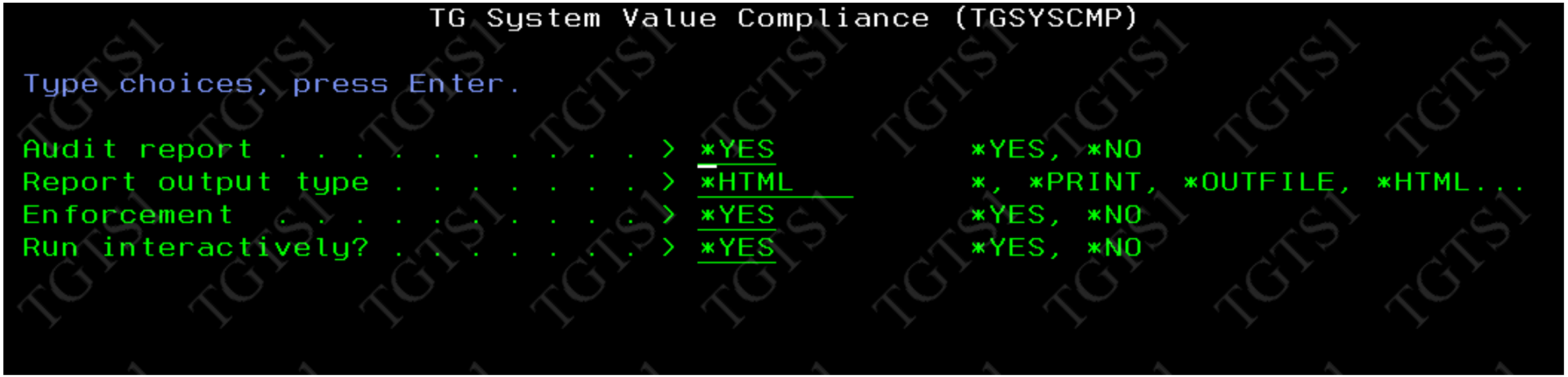
System Value Compliance Status

TGTS1	ALAN	2023-12-11	03:37:52

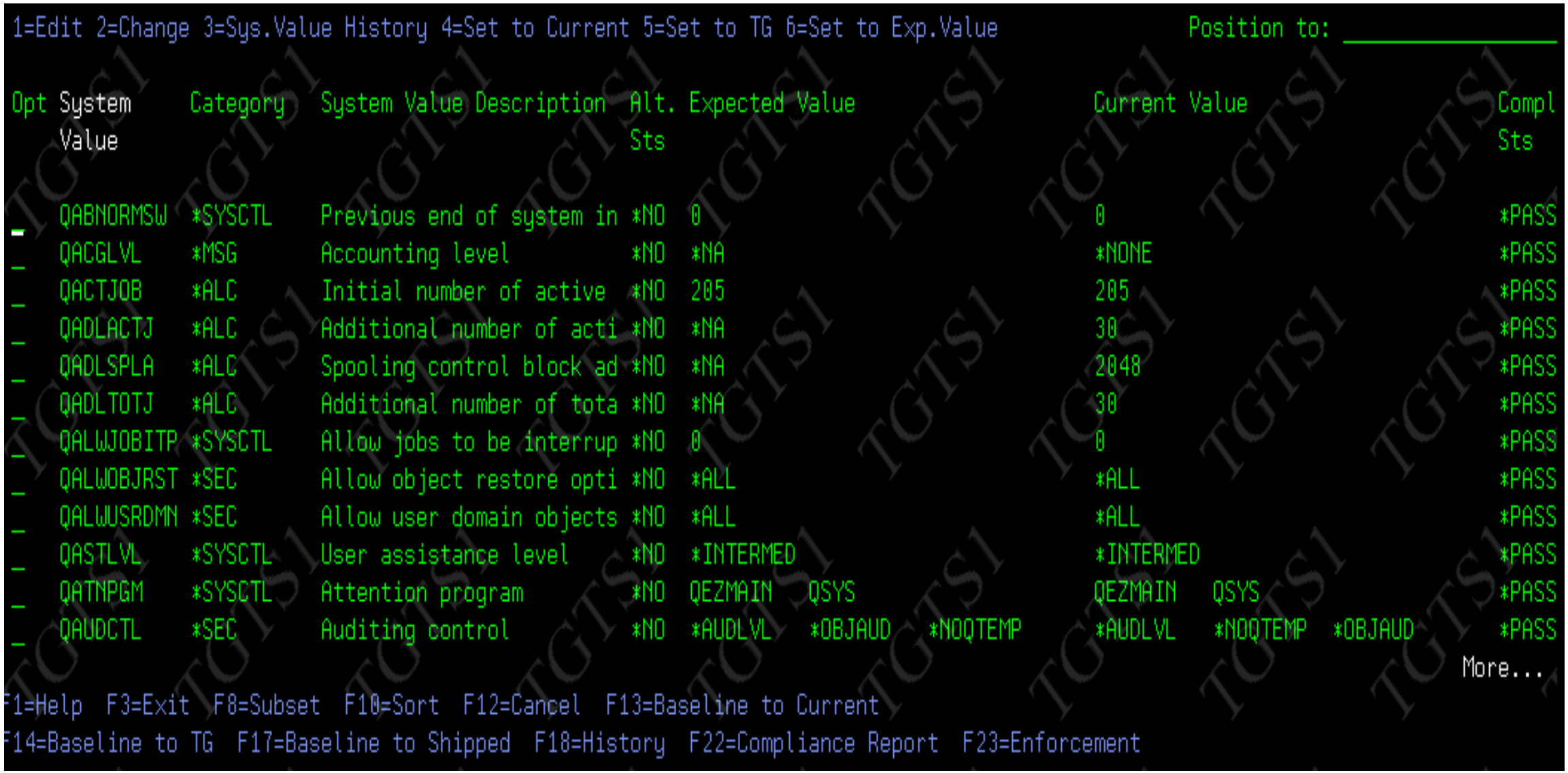
System Value	Category	Description	Compliance Status	
QABNORMSW	*SYSCTL	Previous end of system indicator	*PASS	0
QACGLVL	*MSG	Accounting level	*PASS	*NA
QACTJOB	*ALC	Initial number of active jobs	*FAIL	205
QADLACTJ	*ALC	Additional number of active jobs	*PASS	*NA
QADLSPLA	*ALC	Spooling control block additional storage	*PASS	*NA
QADLTOTJ	*ALC	Additional number of total jobs	*PASS	*NA
QALWJOBITP	*SYSCTL	Allow jobs to be interrupted	*PASS	0
QALWOBJRST	*SEC	Allow object restore option	*PASS	*ALL
QALWUSRDMN	*SEC	Allow user domain objects in libraries	*PASS	*ALL
QASTLVL	*SYSCTL	User assistance level	*PASS	*INTERMED

System Values - Policy

Enforce compliance against System Values policy
TGSYSCMP ARPT(*YES) OUTPUT(*HTML) ENFO(*YES) RUNI(*YES)



System Values - Policy



1=Edit 2=Change 3=Sys.Value History 4=Set to Current 5=Set to TG 6=Set to Exp.Value Position to: _____

Opt	System Value	Category	System Value Description	Alt. Sts	Expected Value	Current Value	Compl Sts
_	QABNORMSW	*SYSCTL	Previous end of system in	*NO	0	0	*PASS
_	QACGLVL	*MSG	Accounting level	*NO	*NA	*NONE	*PASS
_	QACTJOB	*ALC	Initial number of active	*NO	205	205	*PASS
_	QADLACTJ	*ALC	Additional number of acti	*NO	*NA	30	*PASS
_	QADLSPLA	*ALC	Spooling control block ad	*NO	*NA	2048	*PASS
_	QADLTOTJ	*ALC	Additional number of tota	*NO	*NA	30	*PASS
_	QALWJOBITP	*SYSCTL	Allow jobs to be interrup	*NO	0	0	*PASS
_	QALWOBJRST	*SEC	Allow object restore opti	*NO	*ALL	*ALL	*PASS
_	QALWUSRDMN	*SEC	Allow user domain objects	*NO	*ALL	*ALL	*PASS
_	QASTLVL	*SYSCTL	User assistance level	*NO	*INTERMED	*INTERMED	*PASS
_	QATNPGM	*SYSCTL	Attention program	*NO	QEZMAIN QSYS	QEZMAIN QSYS	*PASS
_	QAUDCTL	*SEC	Auditing control	*NO	*AUDLVL *OBJAUD *NOQTEMP	*AUDLVL *NOQTEMP *OBJAUD	*PASS

More...

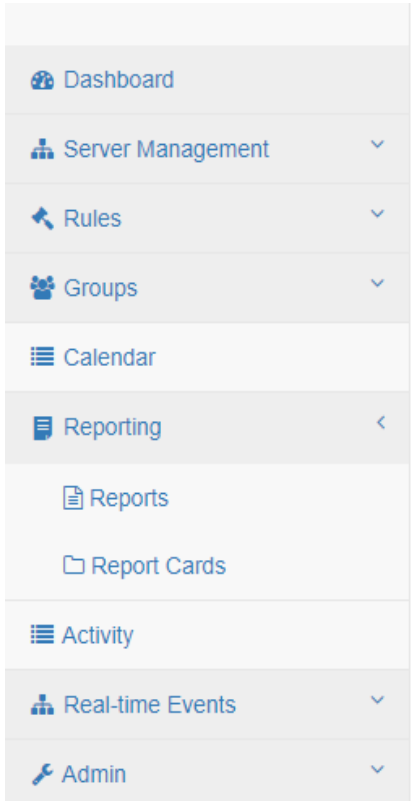
F1=Help F3=Exit F8=Subset F10=Sort F12=Cancel F13=Baseline to Current
F14=Baseline to TG F17=Baseline to Shipped F18=History F22=Compliance Report F23=Enforcement

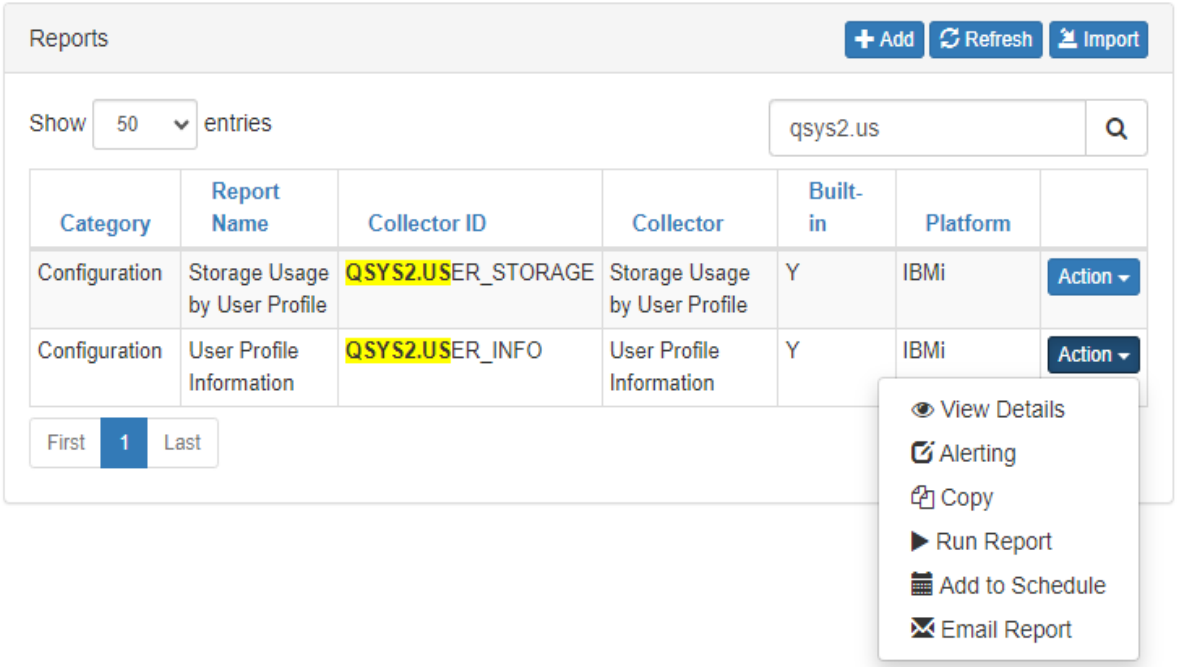
User Profiles

Privileged Users (common to most)

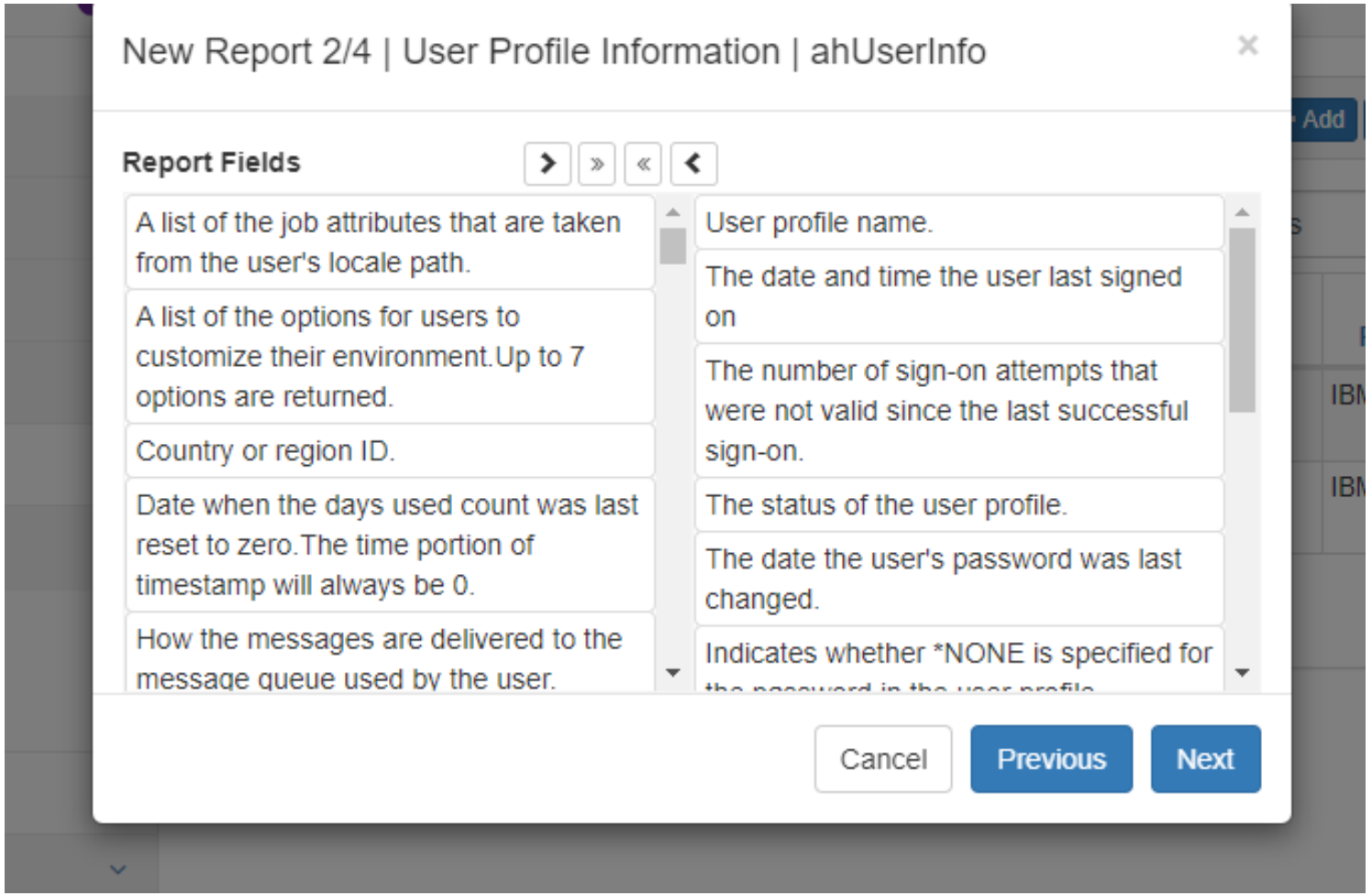
- Special authorities
- Group profiles
- Limited capability

QSYS2.USER_INFO

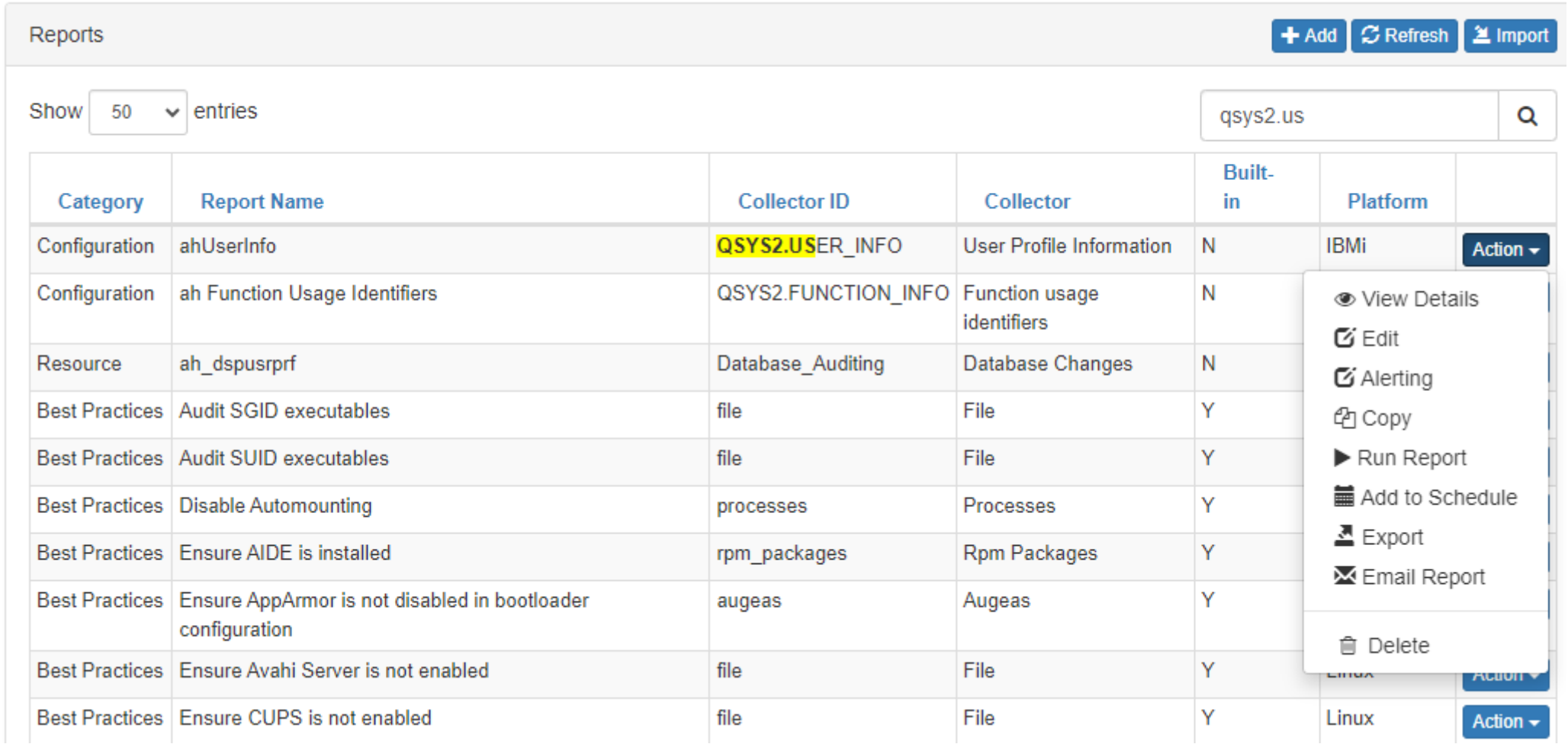




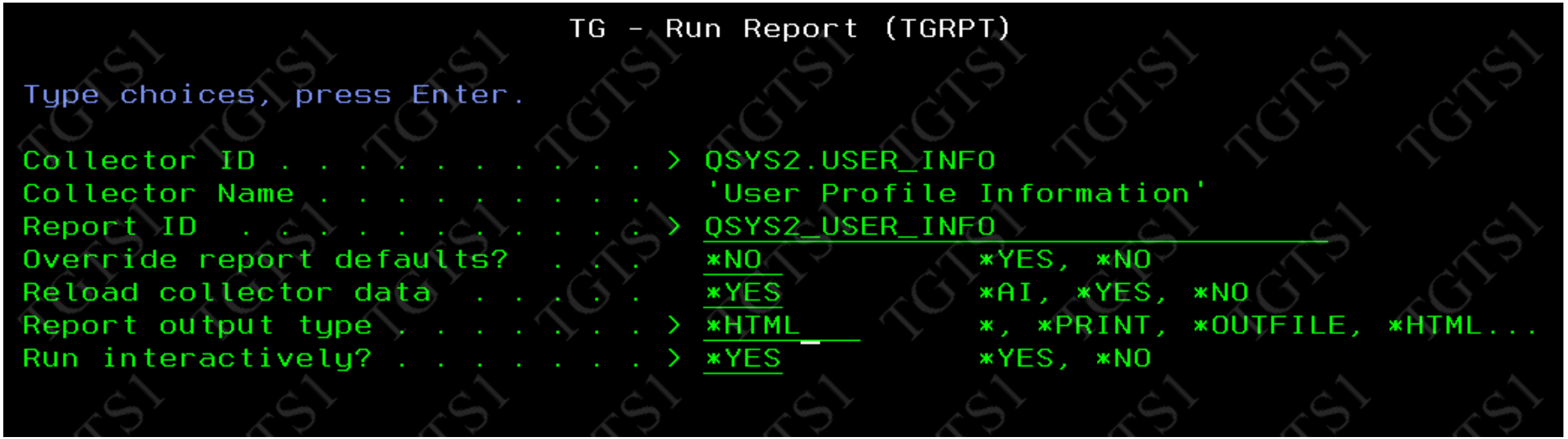
User Profiles



User Profiles



User Profiles



FRESCHE SOLUTIONS

User Profiles

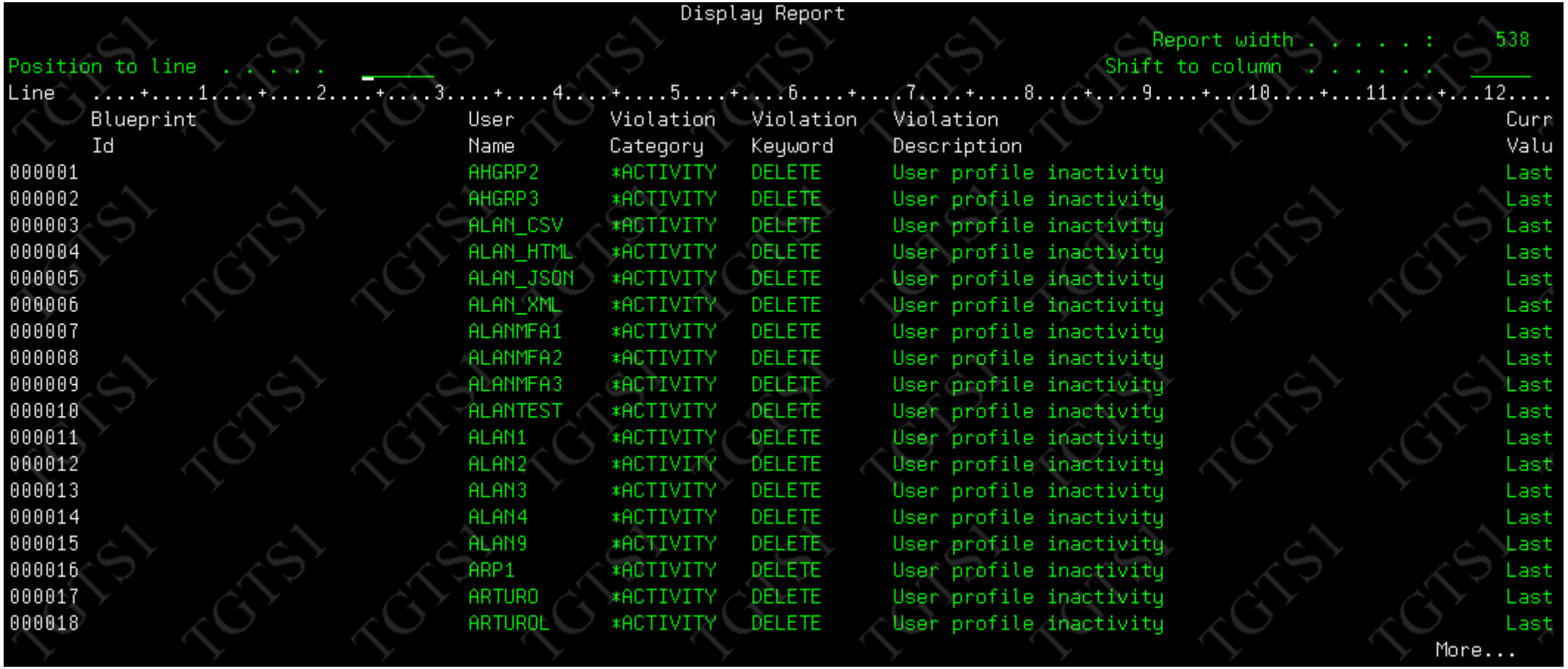
Authorization Name	Previous Signon	Sign On Attempts Not Valid	Status	Password Change	No Password	Password Expiration	Date Password	Days Until Password Expires	Set Password To Expire	User Class	Special Authorities
AHDFTPWD	0001-01-01-00.00.00.000000	0	*DISABLED	2023-11-22-07.42.04.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
AHGRP1	0001-01-01-00.00.00.000000	0	*ENABLED	2022-08-02-09.00.50.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
AHGRP2	0001-01-01-00.00.00.000000	0	*ENABLED	2022-08-02-09.00.55.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
AHGRP3	0001-01-01-00.00.00.000000	0	*ENABLED	2022-08-02-09.00.58.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
AHGRP4	0001-01-01-00.00.00.000000	0	*ENABLED	2022-08-02-09.01.03.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
ALAN	2023-10-04-10.54.44.000000	0	*ENABLED	2022-07-13-11.48.13.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*SECOFR	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG
ALAN_CSV	0001-01-01-00.00.00.000000	0	*DISABLED	2022-08-19-13.14.56.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
ALAN_HTML	0001-01-01-00.00.00.000000	0	*DISABLED	2022-08-19-13.16.30.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
ALAN_JSON	0001-01-01-00.00.00.000000	0	*ENABLED	2022-08-19-13.45.17.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
ALAN_XML	0001-01-01-00.00.00.000000	0	*DISABLED	2022-08-19-13.15.42.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	
ALANMFA	2023-09-15-14.44.14.000000	0	*ENABLED	2023-09-15-10.52.29.000000	NO	0	0001-01-01-00.00.00.000000	0	NO	*USER	

User Profiles

User Profiles

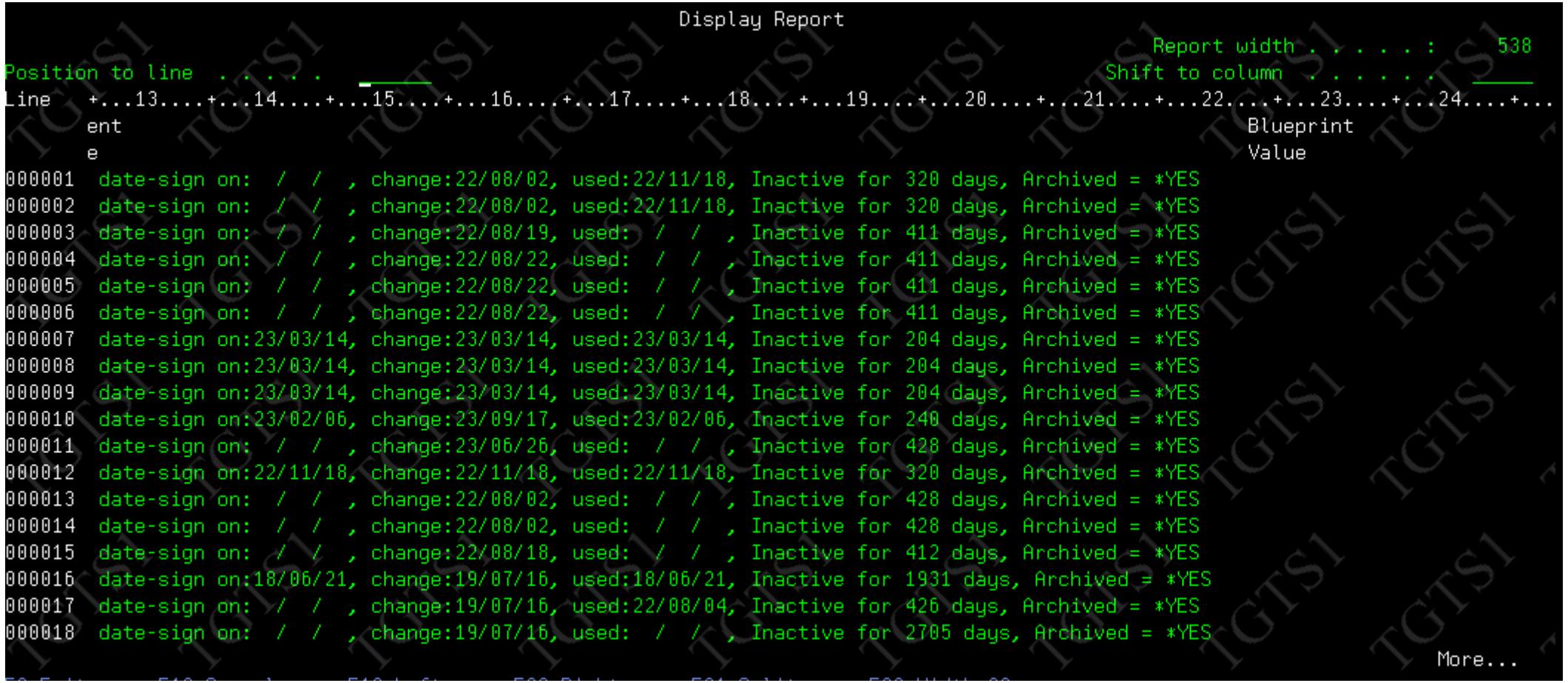
FRESCHE SOLUTIONS

User Profiles



```
                                    Display Report
                                                                  Report width . . . . . :   538
Position to line  . . . . .  _____                              Shift to column  . . . . . .  _____
Line   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12....
       Blueprint                User          Violation   Violation   Violation                                  Curr
       Id                       Name          Category    Keyword     Description                                Valu
000001                          AHGRP2        *ACTIVITY   DELETE      User profile inactivity                    Last
000002                          AHGRP3        *ACTIVITY   DELETE      User profile inactivity                    Last
000003                          ALAN_CSV      *ACTIVITY   DELETE      User profile inactivity                    Last
000004                          ALAN_HTML     *ACTIVITY   DELETE      User profile inactivity                    Last
000005                          ALAN_JSON     *ACTIVITY   DELETE      User profile inactivity                    Last
000006                          ALAN_XML      *ACTIVITY   DELETE      User profile inactivity                    Last
000007                          ALANMFA1      *ACTIVITY   DELETE      User profile inactivity                    Last
000008                          ALANMFA2      *ACTIVITY   DELETE      User profile inactivity                    Last
000009                          ALANMFA3      *ACTIVITY   DELETE      User profile inactivity                    Last
000010                          ALANTEST      *ACTIVITY   DELETE      User profile inactivity                    Last
000011                          ALAN1         *ACTIVITY   DELETE      User profile inactivity                    Last
000012                          ALAN2         *ACTIVITY   DELETE      User profile inactivity                    Last
000013                          ALAN3         *ACTIVITY   DELETE      User profile inactivity                    Last
000014                          ALAN4         *ACTIVITY   DELETE      User profile inactivity                    Last
000015                          ALAN9         *ACTIVITY   DELETE      User profile inactivity                    Last
000016                          ARP1          *ACTIVITY   DELETE      User profile inactivity                    Last
000017                          ARTURO        *ACTIVITY   DELETE      User profile inactivity                    Last
000018                          ARTUROL       *ACTIVITY   DELETE      User profile inactivity                    Last
                                                                                                        More...
```

User Profiles



```
                                    Display Report
                                                                  Report width . . . . . :   538
Position to line  . . . . .  _____                  Shift to column  . . . . . .  ____
Line    +...13....+...14....+...15....+...16....+...17....+...18....+...19....+...20....+...21....+...22....+...23....+...24....+...
        ent                                                                     Blueprint
        e                                                                       Value
000001  date-sign on:  /  /  , change:22/08/02, used:22/11/18, Inactive for 320 days, Archived = *YES
000002  date-sign on:  /  /  , change:22/08/02, used:22/11/18, Inactive for 320 days, Archived = *YES
000003  date-sign on:  /  /  , change:22/08/19, used:  /  /  , Inactive for 411 days, Archived = *YES
000004  date-sign on:  /  /  , change:22/08/22, used:  /  /  , Inactive for 411 days, Archived = *YES
000005  date-sign on:  /  /  , change:22/08/22, used:  /  /  , Inactive for 411 days, Archived = *YES
000006  date-sign on:  /  /  , change:22/08/22, used:  /  /  , Inactive for 411 days, Archived = *YES
000007  date-sign on:23/03/14, change:23/03/14, used:23/03/14, Inactive for 204 days, Archived = *YES
000008  date-sign on:23/03/14, change:23/03/14, used:23/03/14, Inactive for 204 days, Archived = *YES
000009  date-sign on:23/03/14, change:23/03/14, used:23/03/14, Inactive for 204 days, Archived = *YES
000010  date-sign on:23/02/06, change:23/09/17, used:23/02/06, Inactive for 240 days, Archived = *YES
000011  date-sign on:  /  /  , change:23/06/26, used:  /  /  , Inactive for 428 days, Archived = *YES
000012  date-sign on:22/11/18, change:22/11/18, used:22/11/18, Inactive for 320 days, Archived = *YES
000013  date-sign on:  /  /  , change:22/08/02, used:  /  /  , Inactive for 428 days, Archived = *YES
000014  date-sign on:  /  /  , change:22/08/02, used:  /  /  , Inactive for 428 days, Archived = *YES
000015  date-sign on:  /  /  , change:22/08/18, used:  /  /  , Inactive for 412 days, Archived = *YES
000016  date-sign on:18/06/21, change:19/07/16, used:18/06/21, Inactive for 1931 days, Archived = *YES
000017  date-sign on:  /  /  , change:19/07/16, used:22/08/04, Inactive for 426 days, Archived = *YES
000018  date-sign on:  /  /  , change:19/07/16, used:  /  /  , Inactive for 2705 days, Archived = *YES
                                                                                          More...
```

TGTS1

FRESCHE SOLUTIONS

User Profiles – Privileged Access Management

Remove *SECADM, create profile templates/blueprints

Use Case: Restricted User Provisioning without *SECADM
Allow Development manager (ALANNONSEC) the ability to enable their service account (APP01) when needed.

FRESCHE SOLUTIONS

User Profiles – Privileged Access Managment

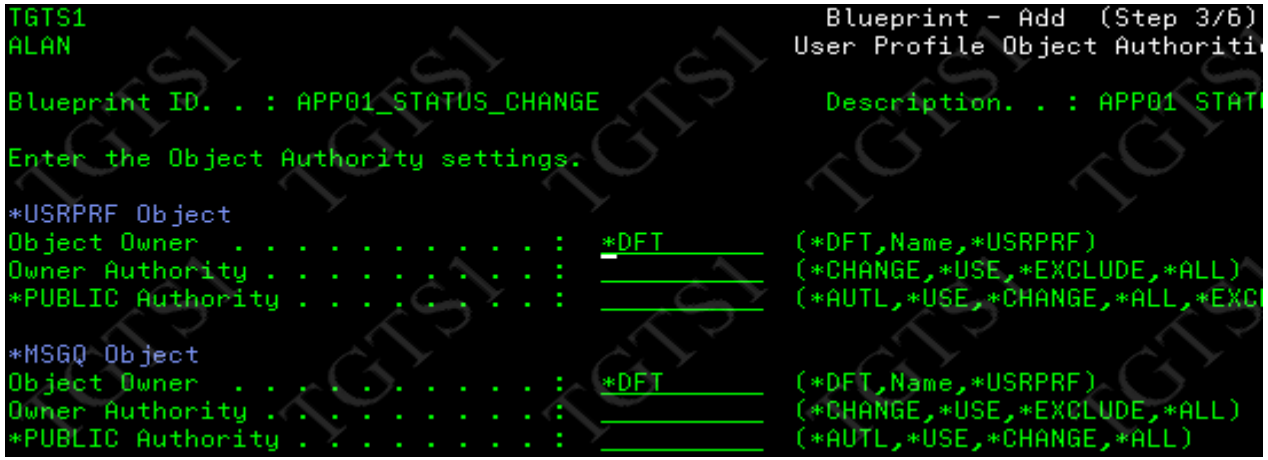
Create Blueprint APP01_STATUS_CHANGE

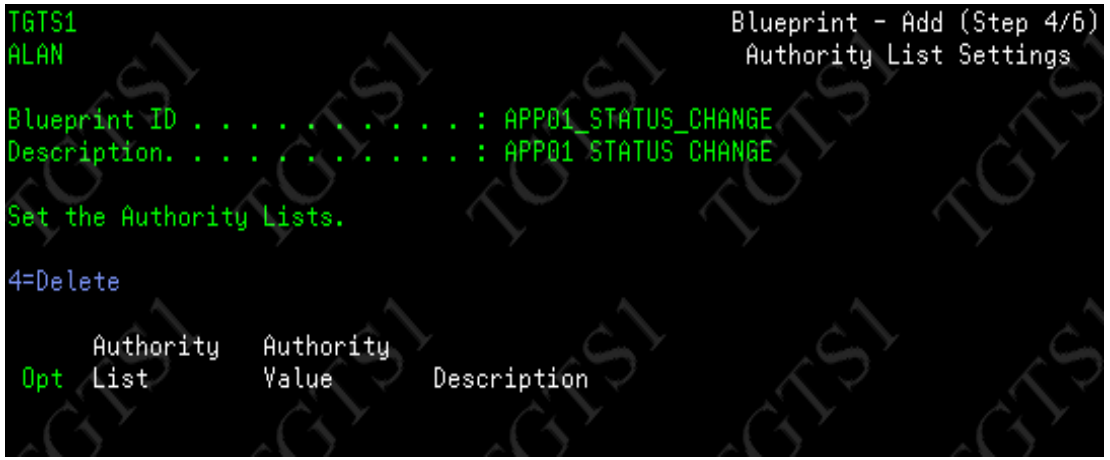
```
TGTS1                                          Blueprint - Add  (Step 1/6)
ALAN

Blueprint details
Blueprint ID. . . . . . . . . . . . . . . . . . . . : APP01_STATUS_CHANGE
Blueprint Description . . . . . . . . . . . . . . . : APP01_STATUS_CHANGE
Alert Status. . . . . . . . . . . . . . . . . . . . : *NO

User Scope. . . . . . . . . . . . . . . . . . . . . : :APP01

Inactivity Overrides
Inactivity until User Profile is disabled (days). . : *DFT
Inactivity until User Profile is deleted  (days). . : *DFT
Object owner for objects owned by deleted profiles. : *DFT
```

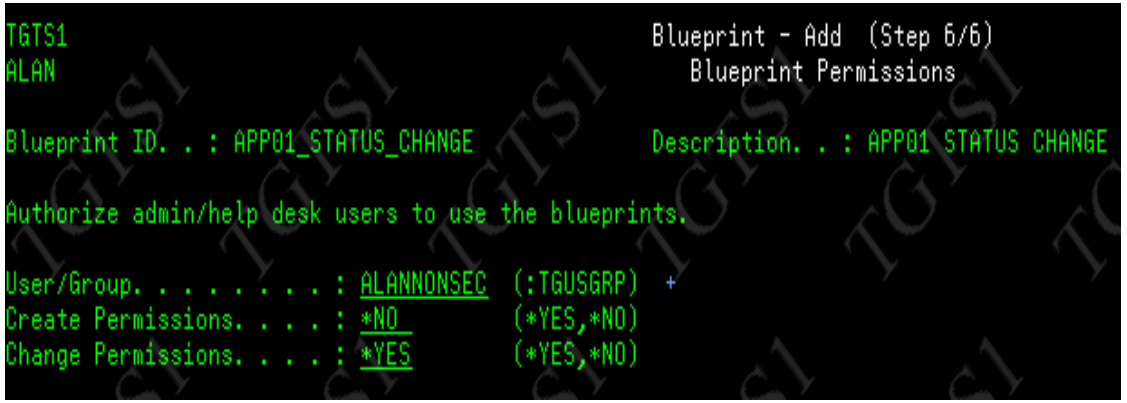
```
TGTS1                                                          Bluepri
ALAN                                                           User Pro

Blueprint ID . . . . . . . . . . . . : APP01_STATUS_CHANGE
Description. . . . . . . . . . . . . : APP01_STATUS_CHANGE

Set the User Profile Parameter values.

4=Delete 2=Edit

Opt Parameter                          Parameter  Parameter
    Description                        keyword    Value

    Status                             STATUS     *ENABLED
```

User Profiles – Privileged Access Management

Create Blueprint APP01_STATUS_CHANGE







User Profiles – Privileged Access Management

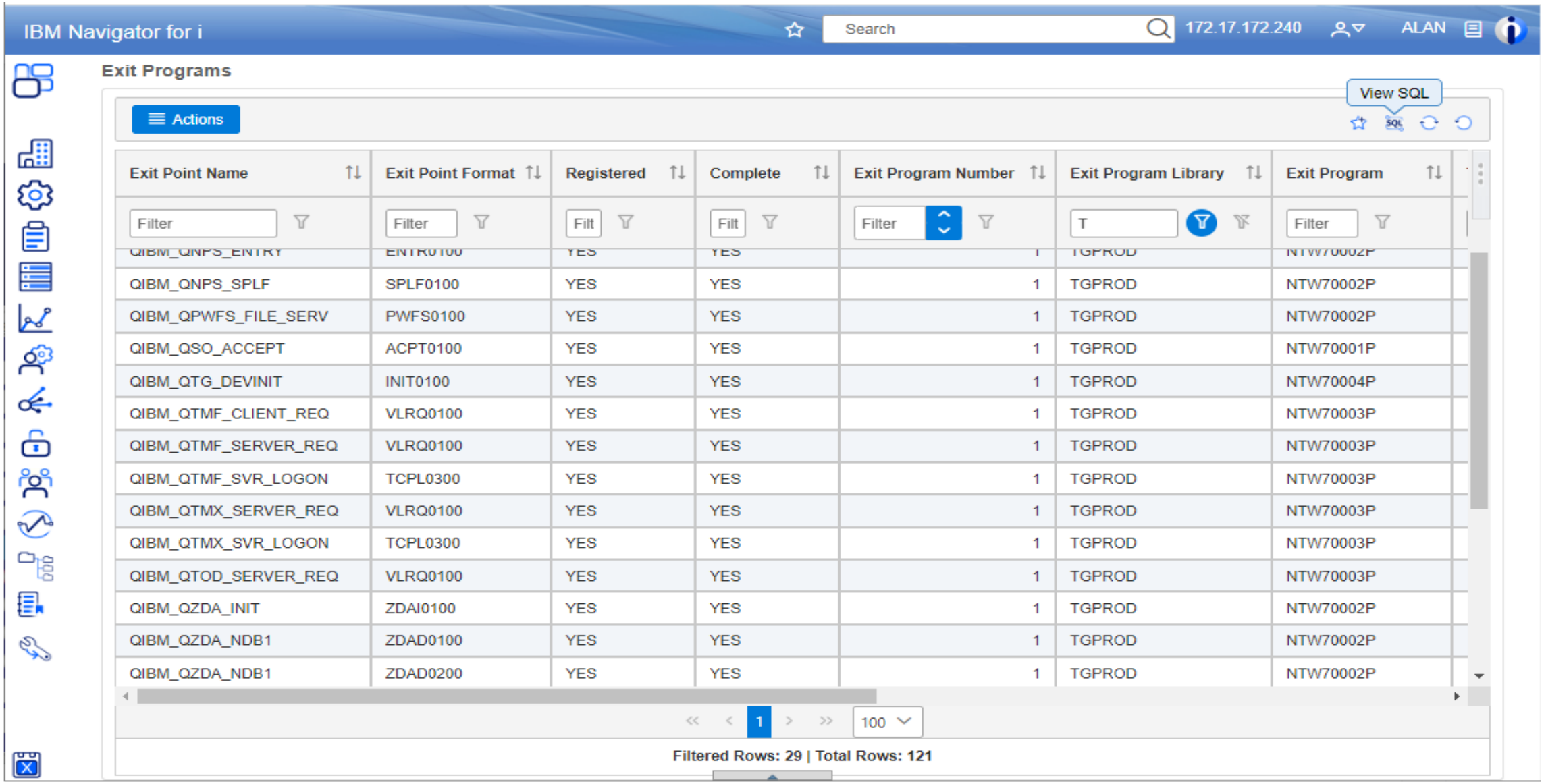
Blueprint APP01_STATUS_CHANGE

Check it out, test it!

TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*NO) RUNI(*YES)

TGPRFCMP COMPN(APP01_STATUS_CHANGE) OUTPUT(*) ENFO(*YES) RUNI(*YES)

Protecting Data – Exit Points



Protecting Data – QSYS

Use QSYS authority schemas

```
Schema ID. . : APP01_QSYS
Description. : APP01_QSYS

2=Edit 3=Copy 4=Delete  5=Display

   File Path or                    Library   Object     Object   Object     Auth       User       Auth       Exception
Opt Sys  ASP                               Name       Type     Owner      List       Object
_  *SYS *SYSBAS                            :APP01              APP01      *NONE      *PUBLIC    *EXCLUDE   *NO
_  *SYS *SYSBAS                            :APP01              APP01      *NONE      APP01      *ALL       *NO
```

```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *USE
```

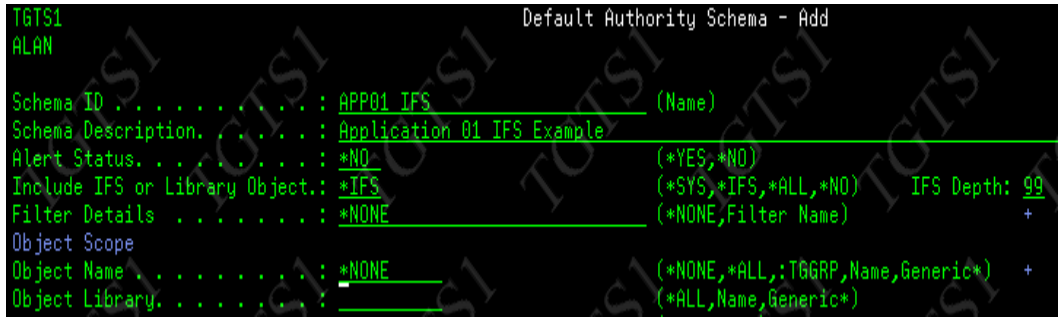
```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : *ALL
Object Library . . . : APP01
Object Type. . . . . : *PGM
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
Adopt User Profile . : *OWNER
Adopt Authority. . . : *YES
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

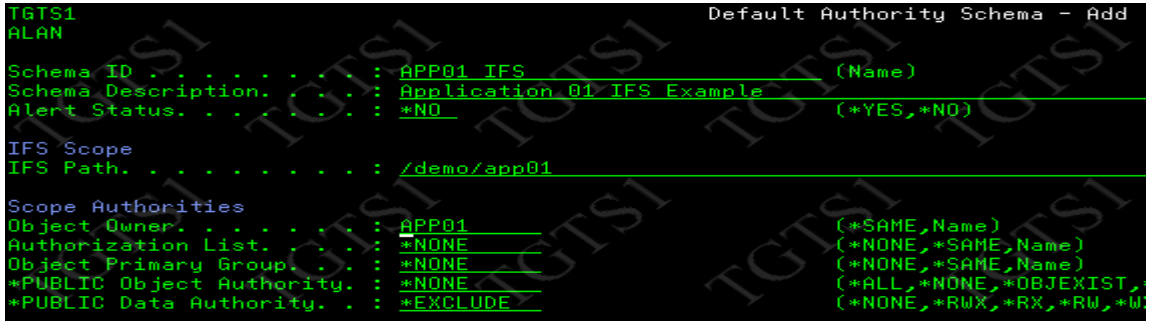
```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *AUTL
```

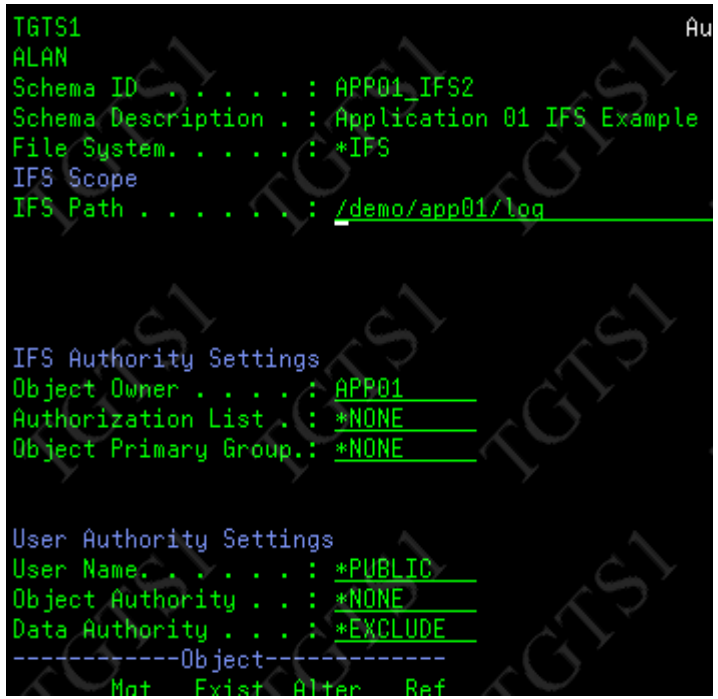
```
Schema ID  . . . . . : APP01_QSYS
Schema Description . : APP01_QSYS
File System. . . . . : *SYS
Object Scope

Object Name. . . . . : APP01
Object Library . . . : QSYS
Object Type. . . . . : *LIB
ASP Name . . . . . : *SYSBAS
Object Authority Settings
Object Owner . . . . : APP01
Authorization List . : APP01
Object Primary Group.: *NONE
Adopt User Profile . : *USER
Adopt Authority. . . : *NO
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
```

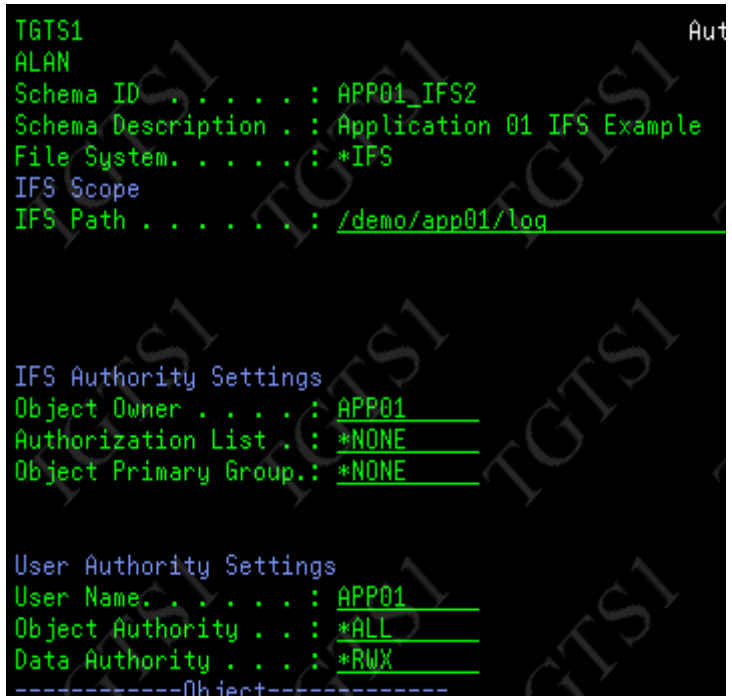
Protecting Data – IFS

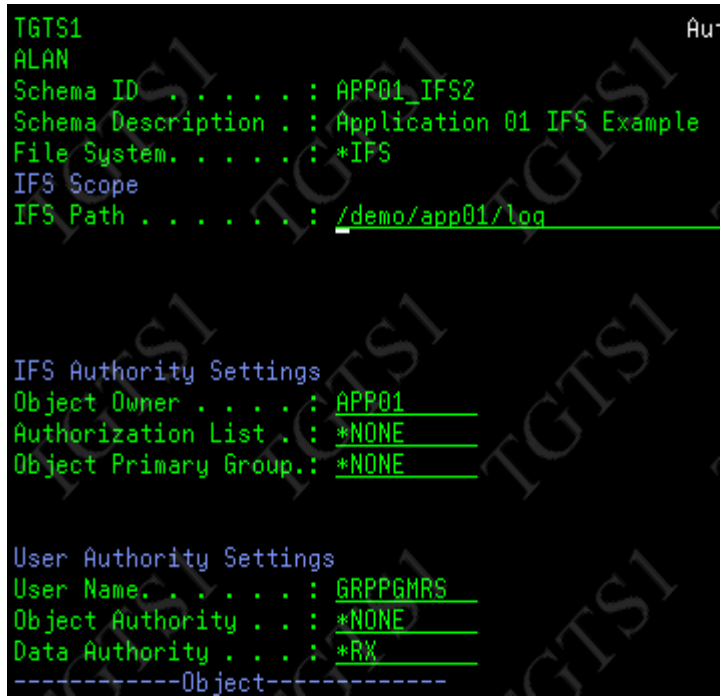
Use IFS authority schemas











Actions to Review from the Audit Journal

Reports

+ Add | Refresh | Import

Show 50 entries

journal_

Category	Report Name	Collector ID	Collector	Built-in	Platform	
Configuration	Object Auditing Attribute Changes	Journal_AD	Object Auditing Attribute Changes	Y	IBMi	Action
Profile	Authority Failures	Journal_AF	Authority Failures	Y	IBMi	Action
Configuration	Programs that Adopt Authority were Executed	Journal_AP	Programs that Adopt Authority were Executed	Y	IBMi	Action
Configuration	EIM Attribute Changes	Journal_AU	EIM Attribute Changes	Y	IBMi	Action
Resource	Row and Column Access Control	Journal_AX	Row and Column Access Control	Y	IBMi	Action
Resource	Advanced Analysis Command Configuration	Journal_C3	Advanced Analysis Command Configuration	Y	IBMi	Action
Profile	Authorization List or Object Authority Changes	Journal_CA	Authorization List or Object Authority Changes	Y	IBMi	Action
Resource	Commands Executed	Journal_CD	Commands Executed	Y	IBMi	Action
Resource	Create Operations	Journal_CO	Create Operations	Y	IBMi	Action
Configuration	User Profile Changes	Journal_CP	User Profile Changes	Y	IBMi	Action
Configuration	Change Request Descriptor Changes	Journal_CQ	Change Request Descriptor Changes	Y	IBMi	Action
Network	Cluster Operations	Journal_CU	Cluster Operations	Y	IBMi	Action
Profile	Connection Verifications	Journal_CV	Connection Verifications	Y	IBMi	Action
Configuration	Cryptographic Configuration Changes	Journal_CY	Cryptographic Configuration Changes	Y	IBMi	Action
Resource	LDAP Operations	Journal_DI	LDAP Operations	Y	IBMi	Action
Resource	Delete Operations	Journal_DO	Delete Operations	Y	IBMi	Action
Profile	Changes to Service Tools Profiles	Journal_DS	Changes to Service Tools Profiles	Y	IBMi	Action

FRESCHE SOLUTIONS

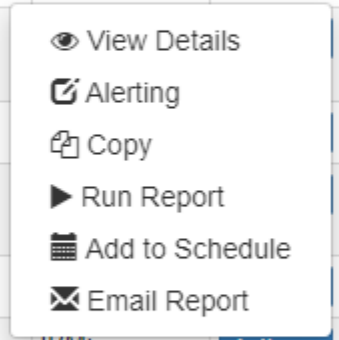
Actions to Review from the Audit Journal – Reports

```
Subset Criteria - Collector ID: *ALL                    Report Type: *BUILT-IN  Category   : *ALL
                  Report Name : *ALL                                            Report ID  : *ALL

1=Sort Fields 2=Edit 3=Copy 4=Delete 5=Alerts 6=Defaults 7=Run 8=Field List 9=Filter    Position to: QSYS

Opt Collector ID                Report Name                                 Report ID                    Category

  _ QSYS2.ACTIVE_JOB_INFO       Active Job Information                      QSYS2_ACTIVE_JOB_INFO        Configurat
  _ QSYS2.DATA_QUEUE_ENTRIES    Data Queue Entries                          DATA_QUEUE_ENTRIES           Resource
  _ QSYS2.DRDA_AUTHENTICATION   DRDA and DDM User Access                    QSYS2_DRDA_AUTHENTICATION    Configurat
  _ QSYS2.EXIT_POINT_INFO       Exit Point Information                      EXIT_POINT_INFO              Configurat
  _ QSYS2.EXIT_PROGRAM_INFO     Exit Program Information                    EXIT_PROGRAM_INFO            Configurat
  _ QSYS2.FUNCTION_INFO         Function Usage Identifiers                  QSYS2_FUNCTION_INFO          Configurat
  _ QSYS2.FUNCTION_USAGE        Function Usage Configuration Details        QSYS2_FUNCTION_USAGE         Configurat
  _ QSYS2.GROUP_PTF_INFO        Group PTFs Information                      QSYS2_GROUP_PTF_INFO         Configurat
  _ QSYS2.JOURNAL_INFO          Journal and Remote Journal Information      QSYS2_JOURNAL_INFO           Configurat
  _ QSYS2.JOURNALED_OBJECTS     Journaled Objects                           JOURNALED_OBJECTS            Resource
  _ QSYS2.LICENSE_INFO          Products License Information                QSYS2_LICENSE_INFO           Configurat
  _ QSYS2.MEDIA_LIBRARY_INFO    Media Library Status Details                QSYS2_MEDIA_LIBRARY_INFO     Configurat
                                                                                                          More...

F1=Help  F3=Exit  F6=Add Report  F8=Subset  F10=Sort  F11=Report Type  F12=Cancel
```

FRESCHE SOLUTIONS

Actions to Review from the Audit Journal – Reports

Configuration	Active Job Information	QSYS2.ACTIVE_JOB_INFO	Active job information	Y	IBMi	Action
Resource	Data Queue Entries	QSYS2.DATA_QUEUE_ENTRIES	Data Queue Entries	Y	IBMi	Action
Configuration	DRDA and DDM User Access	QSYS2.DRDA_AUTHENTICATION	DRDA and DDM User Access	Y	IBMi	Action
Configuration	Exit Point Information	QSYS2.EXIT_POINT_INFO	Exit Point Information	Y	IBMi	Action
Configuration	Exit Program Information	QSYS2.EXIT_PROGRAM_INFO	Exit Program Information	Y	IBMi	Action
Configuration	Function Usage Identifiers	QSYS2.FUNCTION_INFO	Function usage identifiers	Y	IBMi	Action
Configuration	Function Usage Configuration Details	QSYS2.FUNCTION_USAGE	Function Usage Configuration Details	Y		
Configuration	Group PTFs Information	QSYS2.GROUP_PTF_INFO	Group PTFs Information	Y		
Configuration	Journal and Remote Journal Information	QSYS2.JOURNAL_INFO	Journal and Remote Journal Information	Y		
Resource	Journaled Objects	QSYS2.JOURNALED_OBJECTS	Journaled Objects	Y		
Configuration	Products License Information	QSYS2.LICENSE_INFO	Products License Information	Y	IBMi	Action
Configuration	Media Library Status Details	QSYS2.MEDIA_LIBRARY_INFO	Media Library Status Details	Y	IBMi	Action
Configuration	Memory Pool Details	QSYS2.MEMORY_POOL	Memory Pool Details	Y	IBMi	Action
Configuration	Message Queue Data by Date range	QSYS2.MESSAGE_QUEUE_INFO	Message Queue Data by Date range	Y	IBMi	Action
Configuration	IPv4 and IPv6 Network Connection Details	QSYS2.NETSTAT_JOB_INFO	IPv4 and IPv6 Network Connection Details	Y	IBMi	Action



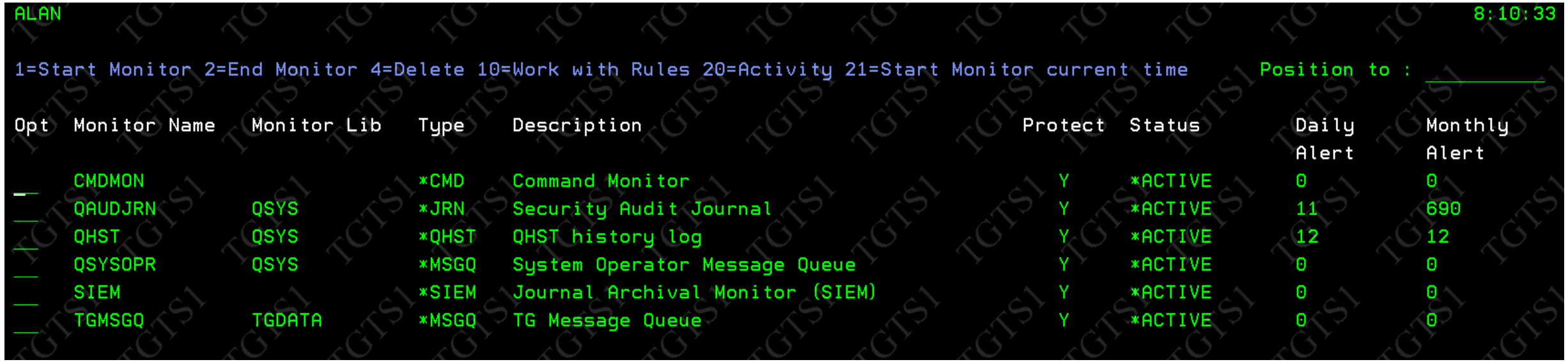
FRESCHE SOLUTIONS

Actions to review from the Audit Journal – Report Cards

TGFree Security Assessment | Analysis

#	Category	Report Name	Regulation Clause	Pass Criteria	Number of Rows
1	Resource	Authorization Lists with Public Access		<	1
2	Profile	Group Profiles with Passwords		<	1
3	Resource	Integrated File System Security		<	1
4	Network	NetServer shares		<	1
5	Network	Network Connection Details		INFO	0
6	Profile	User Profiles Not Used in 90 Days		<	1
7	Profile	Powerful User Profiles		<	4
8	Profile	User Profile = Password		<	1
9	Resource	Allow Object Restore Option		<	1
10	Resource	Allow User Domain Objects in Libraries		<	1
11	Configuration	System, User, and Object Auditing Control Configuration		<	1
12	Configuration	Attention Events are Audited		>	0
13	Configuration	Authorization Failures are Audited		>	0
14	Configuration	All Object Creations are Audited		>	0
15	Configuration	All Deletions of External Objects on the System are Audited		>	0
16	Configuration	Actions that Affect a Job are Audited		>	0

Evidence - Supporting Documentation - Reporting



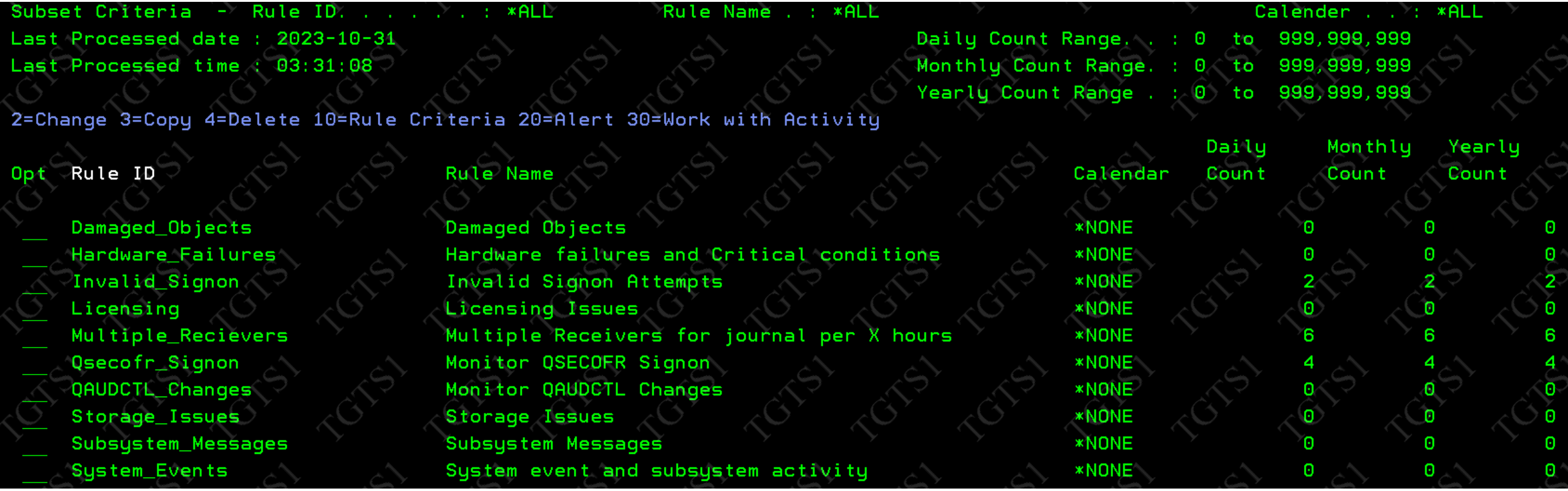
ALAN 8:10:33

1=Start Monitor 2=End Monitor 4=Delete 10=Work with Rules 20=Activity 21=Start Monitor current time Position to :

Opt	Monitor Name	Monitor Lib	Type	Description	Protect	Status	Daily Alert	Monthly Alert
	CMDMON		*CMD	Command Monitor	Y	*ACTIVE	0	0
	QAUDJRN	QSYS	*JRN	Security Audit Journal	Y	*ACTIVE	11	690
	QHST	QSYS	*QHST	QHST history log	Y	*ACTIVE	12	12
	QSYSOPR	QSYS	*MSGQ	System Operator Message Queue	Y	*ACTIVE	0	0
	SIEM		*SIEM	Journal Archival Monitor (SIEM)	Y	*ACTIVE	0	0
	TGMSGQ	TGDATA	*MSGQ	TG Message Queue	Y	*ACTIVE	0	0

FRESCHE SOLUTIONS

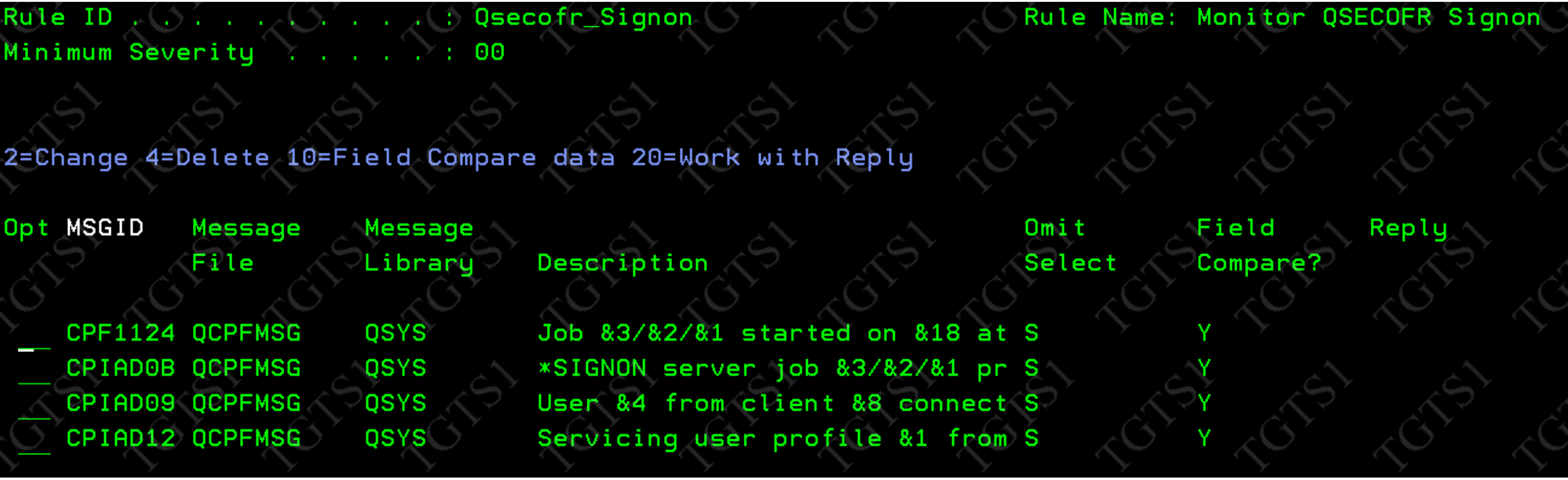
Evidence - Supporting Documentation - Reporting



```
Subset Criteria  -  Rule ID. . . . . : *ALL        Rule Name . : *ALL                          Calender . . : *ALL
Last Processed date : 2023-10-31                                  Daily Count Range. . : 0  to  999,999,999
Last Processed time : 03:31:08                                    Monthly Count Range. : 0  to  999,999,999
                                                                  Yearly Count Range . : 0  to  999,999,999
2=Change 3=Copy 4=Delete 10=Rule Criteria 20=Alert 30=Work with Activity

                                                                                  Daily     Monthly   Yearly
Opt  Rule ID                    Rule Name                                         Calendar  Count     Count     Count

__   Damaged_Objects            Damaged Objects                                   *NONE             0         0         0
__   Hardware_Failures          Hardware failures and Critical conditions         *NONE             0         0         0
__   Invalid_Signon             Invalid Signon Attempts                           *NONE             2         2         2
__   Licensing                  Licensing Issues                                  *NONE             0         0         0
__   Multiple_Recievers         Multiple Receivers for journal per X hours        *NONE             6         6         6
__   Qsecofr_Signon             Monitor QSECOFR Signon                            *NONE             4         4         4
__   QAUDCTL_Changes            Monitor QAUDCTL Changes                           *NONE             0         0         0
__   Storage_Issues             Storage Issues                                    *NONE             0         0         0
__   Subsystem_Messages         Subsystem Messages                                *NONE             0         0         0
__   System_Events              System event and subsystem activity               *NONE             0         0         0
```

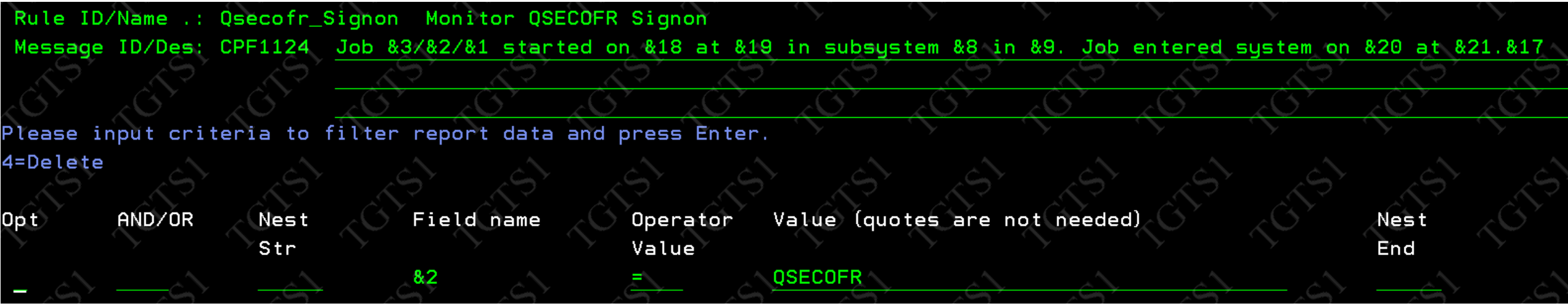
FRESCHE SOLUTIONS

Evidence - Supporting Documentation - Reporting



```
Rule ID . . . . . : Qsecofr_Signon                    Rule Name: Monitor QSECOFR Signon
Minimum Severity  . . . . . : 00


2=Change 4=Delete 10=Field Compare data 20=Work with Reply

Opt MSGID   Message    Message                                    Omit      Field     Reply
            File       Library    Description                     Select    Compare?

 _  CPF1124 QCPFMSG    QSYS       Job &3/&2/&1 started on &18 at  S         Y
 _  CPIAD0B QCPFMSG    QSYS       *SIGNON server job &3/&2/&1 pr  S         Y
 _  CPIAD09 QCPFMSG    QSYS       User &4 from client &8 connect  S         Y
 _  CPIAD12 QCPFMSG    QSYS       Servicing user profile &1 from  S         Y
```

Evidence - Supporting Documentation - Reporting



TGTS1

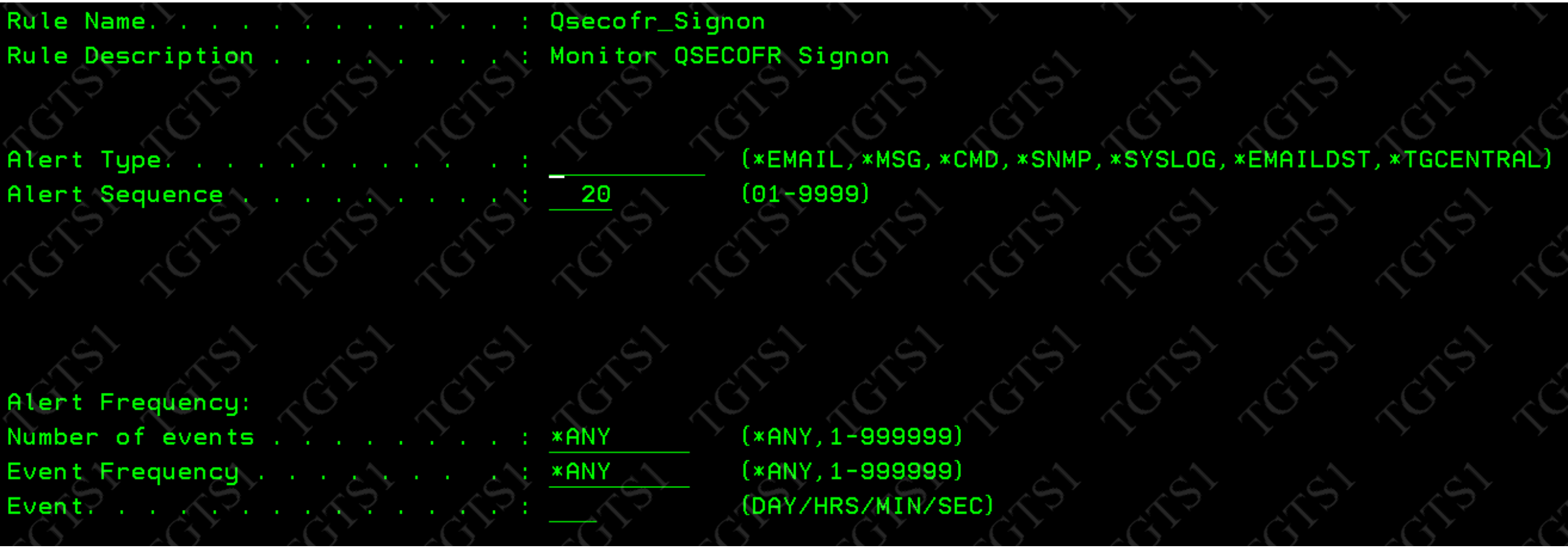
FRESCHE SOLUTIONS

Evidence - Supporting Documentation - Reporting

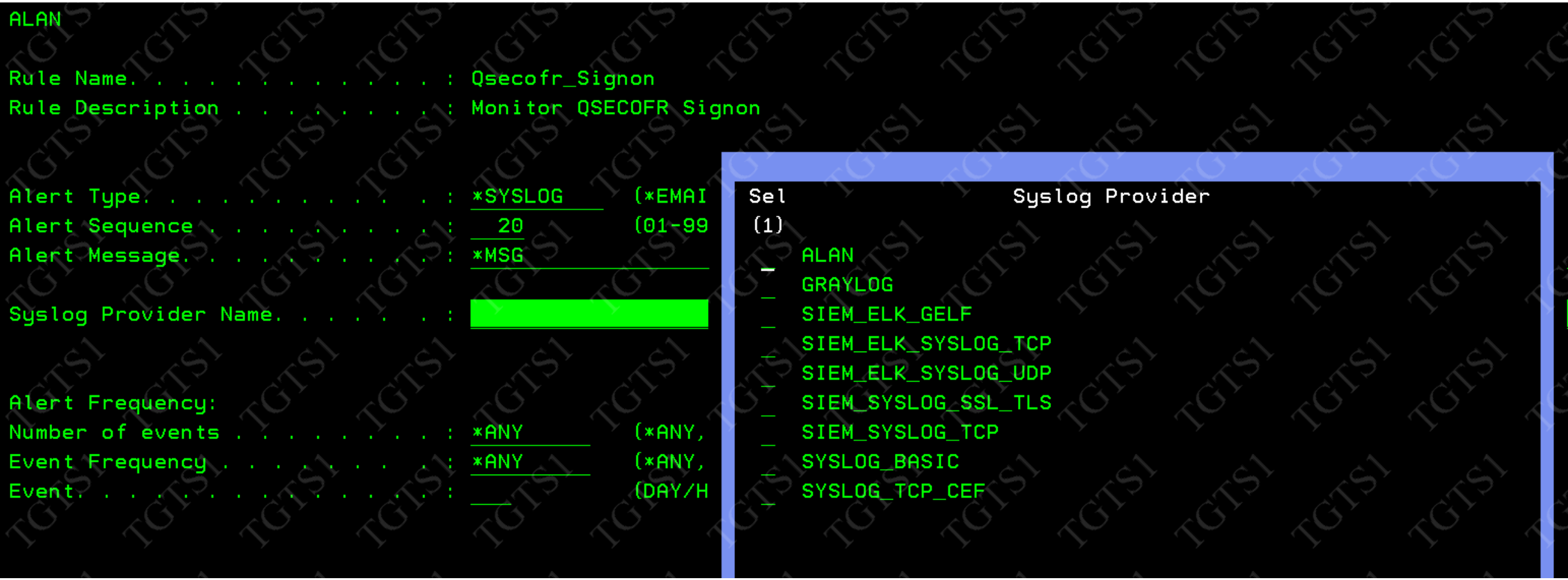
TGTS1

FRESCHE SOLUTIONS

Evidence - Supporting Documentation - Reporting



Evidence - Supporting Documentation - Reporting



Evidence - Supporting Documentation - Reporting

- Dashboard
- Server Management
- Rules
- Groups
- Calendar
- Reporting
  - Reports
  - Report Cards
- Activity
- Real-time Events
  - Network Activity
  - Alert
- Admin

Alerts

Email Config | Reset Filter | Filter | Refresh(48)

Show 50 entries

Search

Server	Facility	Job Number	Message	Message ID	Severity	Timestamp	Type	Version	Show
TGSE1.TRINITYGUARD.COM	Log alert	381099/QSYS/QDBSRV02	Sequence number not reset. First sequence number is 7457031.	CPF7019	informational	2023-11-05-02.02.12	syslog	1	
TGSE1.TRINITYGUARD.COM	Log alert	381099/QSYS/QDBSRV02	Journal receiver AUDRCV0346 created in library QGPL.	CPC7011	informational	2023-11-05-02.02.12	syslog	1	
TGSE1.TRINITYGUARD.COM	Log alert	381099/QSYS/QDBSRV02	Sequence number not reset. First sequence number is 6426901.	CPF7019	informational	2023-10-21-19.44.45	syslog	1	
TGSE1.TRINITYGUARD.COM	Log alert	381099/QSYS/QDBSRV02	Journal receiver AUDRCV0345 created in library QGPL.	CPC7011	informational	2023-10-21-19.44.45	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	609505/AVG/QPADEV0001	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-09-05-15.14.31	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	609490/AVG/QPADEV0001	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-09-05-14.17.41	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	609490/AVG/QPADEV0001	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-09-05-14.12.03	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	607077/AVG/QPADEV0002	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-08-16-22.39.02	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	587468/AVG/QPADEV000K	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-07-17-15.46.21	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	528521/AVG/QPADEV0004	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-07-12-17.10.27	syslog	1	
TGDEV4.pepitoYGUARD.COM	Log alert	528571/AVG/QPADEV000N	Command STRSQL was executed by User AVG	QSQL/STRSQL	informational	2023-07-12-15.06.50	syslog	1	

Poll Question: What challenges are you currently facing in securing your IBM i?

FRESCHE SOLUTIONS

IT & IBM i experts providing solutions to design, develop, modernize, transform & secure business-critical systems and deliver results!

IT & Technology Advisory

Establish a forward-thinking IT strategy and IBM i modernization roadmap aligned with business direction.

Modernization

Improve business process with application and DB conversion to modern languages and architectures, new development, integration, APIs and digital enablement.

Cloud

Move IBM i applications & create powerful new workloads for development, testing, archive, backup and HA.

Data

Build better applications, reporting, and turn data into intelligence (analytics, modernization, AI).

Security & Compliance

Guard against cyber threats with security solutions that protect you at every level - IFS, SIEM integration, encryption & MFA.

Managed Services

Manage, optimize, and evolve IT with full-stack and IBM i experts to support your critical IBM i applications, ERP systems & infrastructure.

Next Steps…

- Download a Free Trial
- Subscribe to Fresche Security
- Speak with a security expert
- Ask about pen testing

Questions?

alan.hamm@freschesolutions.com

info@freschesolutions.com

FRESCHE SOLUTIONS