

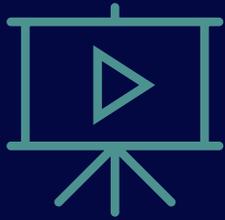
# Top 5 Tasks for IBM i Admins

---

FRESCHESOLUTIONS



# Housekeeping



Get the slides & session  
recording via email



Ask questions



Share your thoughts



**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

IBMCHAMPION 

[carol@dxrsecurity.com](mailto:carol@dxrsecurity.com)



# Why are We Talking About This?

When security is not administered, it typically becomes  
'undone.'

# 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\*



# User Profiles

# Reviewing User Profile Capabilities

- Group profile assignments
- Special authorities
- Limited capability setting

# 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

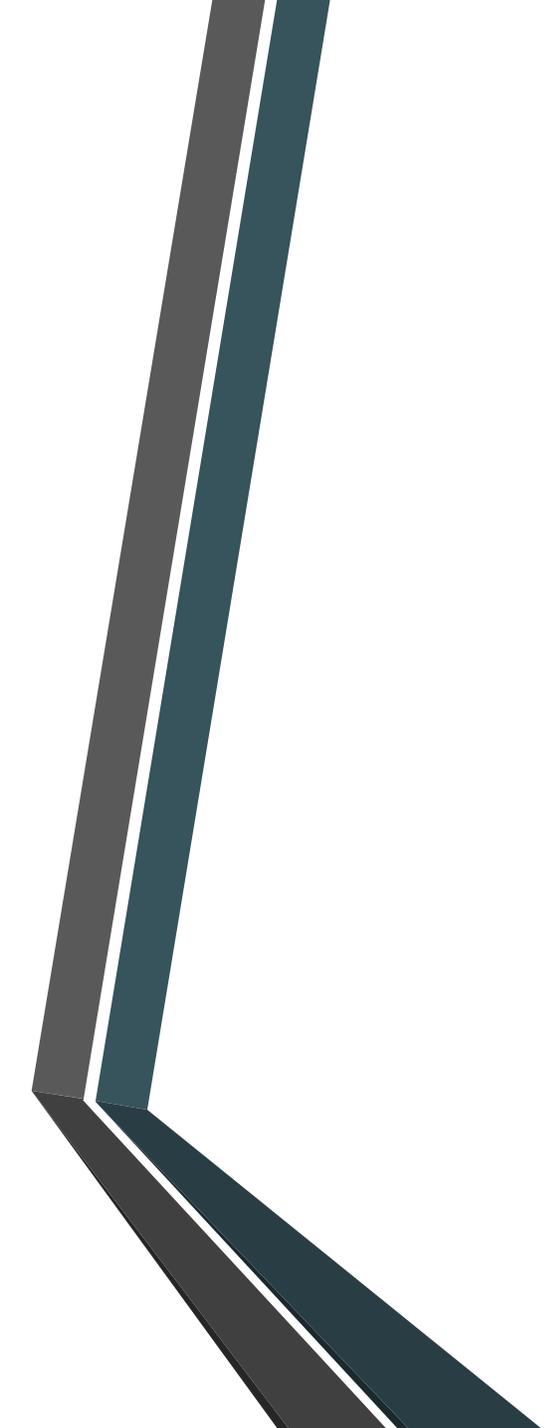
# Service Account Setting Recommendations

- 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.

# 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)



# Protecting Data



# Working with System Values

Security Configuration Information 

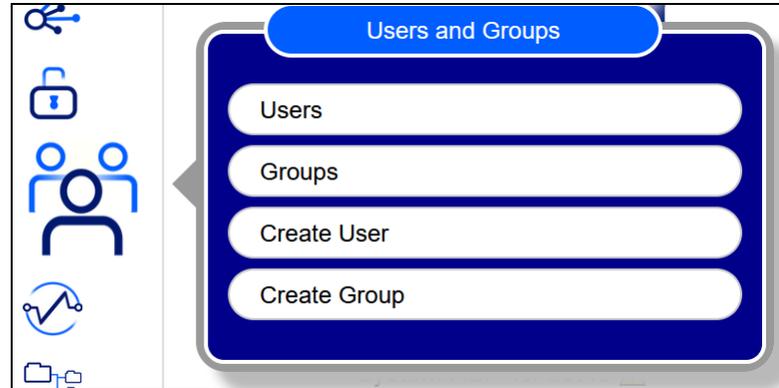
Actions

Name ↑↓	Current Value ↑↓	Values ↑↓	Description ↑↓
audit	Filter	Filter	Filter
Auditing Control	*AUDLVL *OBJAUD *NOQTEMP	*NOTAVL, *NONE, *OBJAUD, *AUDLVL, *NOQTEMP	The current setting for the auditing control system value
Auditing Level	*AUDLVL2	*NONE, *AUDLVL2	The current setting for the auditing level value
Auditing Level Extension	*AUTFAIL *NETFAIL *PGMFAIL *SECCFG *SECRUN *SERVICE *NETSECURE*CREATE	*NONE, *NOTAVL, *ATNEVT, *AUTFAIL, *CREATE, *DELETE, *JOBBAS, *JOBCHGUSR, *JOBDDTA, *NETBAS, *NETCLU, *NETCMN, *NETFAIL, *NETSCK, *OBJMGT, *OFCSRVR, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDDTA, *PTFOBJ, *PTFOPR, *SAVRST, *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECCKD, *SECURITY, *SECVFY, *SECVLDL, *SERVICE, *SPLFDTA, *SYSMGT	The current setting for the auditing level (QAUDLVL2) system value
Audit Journal Receiver Library	QAUDRCV		The name of the library that contains the attached to the security journal
Audit Journal Receiver	AUDRCV1346		The name of the journal receiver attached to the security journal

Navigation: << < 1 > >> 500

[http://your\\_system\\_name:2002/Navigator/login](http://your_system_name:2002/Navigator/login)

# 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	Status	Password Expiration Interval	Special Authorities	Group Profile Name	Supplemental Group List	Last Used Timestamp
USER_NAME	STATUS	PASSWORD_EXPIRATION_INTERVAL	SPECIAL_AUTHORITIES	GROUP_PROFILE_NAME	SUPPLEMENTAL_GROUP_LIST	LAST_USED_TIMESTAMP
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 00:00:00.0000

## 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

# 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				Status	Text Description
USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	STATUS	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!

# 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

# 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.

## 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)

# Fresche Security – The GUI

**TGCENTRAL** Show ▾ [en] ? ADMIN ▾

- Dashboard
- Server Management ▾
- Rules ▾
- Groups ▾
- Calendar
- Reporting ▾
- Activity
- Real-time Events ▾
- Admin ▾

**0**  
0% Since last Month  
Reports Run

**3**  
▼1033% Since last Month  
Report Cards Run

**0**  
0% Since last Month  
Empty Reports

**0**  
0% Since last Month  
Error Reports

**Statistics of Reports**

Month	Blue Line	Green Area
2022-10	0	0
2022-11	10	15
2022-12	0	5
2023-01	0	5
2023-02	0	10
2023-03	0	0
2023-04	10	15
2023-05	5	35
2023-06	0	40
2023-07	0	35
2023-08	0	35
2023-09	0	35
2023-10	0	0

**Activity History**

- User Login ADMIN 09:09
- Server TGSE1.TRINITYGUARD.COM edited 00:21
- Network Security Defaults imported 00:21
- Access Escalation Defaults imported 00:21
- Inactive Session Lockdown Defaults imported 00:21
- Resource Manager Defaults imported 00:21

# Fresche Security – The GUI

The screenshot displays the TG CENTRAL web interface. The top navigation bar includes the logo, language settings ([en]), a help icon, and the user name (ADMIN). A left-hand sidebar menu lists various system components, with 'Rules' expanded to show 'Remote Exit Rules' selected. The main content area is titled 'Remote Exit Rules' and features '+ Add' and 'Refresh' buttons. Below the title, there is a 'Show 50 entries' dropdown and a search box. The central part of the interface is a table listing 15 remote exit rules. Each row contains columns for Server, User/Group, Operation Server, Function, Client IP, Calendar, Alert Status, Exit Rule Action, Object Details, and an Action button. The table is currently on page 1 of 1.

Server	User/Group	Operation Server	Function	Client IP	Calendar	Alert Status	Exit Rule Action	Object Details	Action
TGSE1.TRINITYGUARD.COM	*PUBLIC	*ALL		*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.11.12.35	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.32	*NONE	*YES	*PASS		Action
*ALL	*PUBLIC	*ALL		*ALL	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	*ALL	10.11.12.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	:ADMIN	FILE	*ALL	10.*	*NONE	*NO	*PASS	/home/PMB/mydir	Action
TGSE1.TRINITYGUARD.COM	PMB	DBSQL	*ALL	10.*	*NONE	*NO	*PASS	FINANCE/CUSTMAST.FILE	Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	*ALL	10.27.*	*NONE	*NO	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	DBSQL	*ALL	10.27.81.26	*NONE	*YES	*PASS	FINANCE/CUSTMAST.FILE	Action
TGSE1.TRINITYGUARD.COM	:ADMIN	FTPSRV	LOGON	10.11.*	*NONE	*YES	*PASS		Action
TGSE1.TRINITYGUARD.COM	PMB	:FILEGRP		10.27.81.30	*NONE	*NO	*PASS	/TrinityGuard/Reports	Action
TGSE1.TRINITYGUARD.COM	PMB	FTPSRV	LOGON	10.27.81.23	*NONE	*YES	*FAIL		Action

# Fresche Security – The GUI

The screenshot shows the TGCENTRAL web interface. The top navigation bar includes the logo, language selection ([en]), a help icon, and the user name ADMIN. The left sidebar contains a menu with items: Dashboard, Server Management, Servers, Server Groups, Rules, Groups, Calendar, Reporting, Reports, Report Cards, Activity, Real-time Events, and Admin. The main content area is titled 'List of Roles' and features '+ Add' and 'Refresh' buttons. Below the title, there is a 'Show 50 entries' dropdown and a search box. The table below lists the roles:

Name	Description	Built-in	Functions
Admin	Power user with access to all Functionality	Yes	Action
Auditor	Ability to create, view, run, and rerun reports. Auditor has the ability to view rules (ie JAM), but not change or delete them.	Yes	Action
Creator	Responsible for creating reports, and should also have everything that a Reader has.	Yes	Action
Helpdesk	Usually helps users troubleshoot issues with their reports, or logging in, etc. Hence they can generally do everything an Auditor can do, and actions to users, except delete them.	Yes	Action
Reader	Ability to view reports and delta reports.	Yes	Action
Super User	Everything the Help Desk has, plus the ability to maintain rules and delete users. This would be the equivalent of the Admin, minus Rules, and Settings.	Yes	Action

At the bottom of the table, there is a pagination control showing 'First 1 Last'.

# 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 *JOBDDTA *NETCMN *NETSCK *NETTELSVR *NETUDP *OBJMGT *OFCSRVR *OPTICAL *PGMADP *PGMFAIL *PRTDDTA *PTFOBJ *PTFOPR *SAVRST *SECURITY *SERVICE *SPLFDDTA *SYSMGT	*NONE, *NOTAVL, *ATNEVT, *AUTFAIL, *CREATE, *DELETE, *JOBDDTA, *JOBCHGUSR, *JOBDDTA, *NETBAS, *NETCLU, *NETCMN, *NETFAIL, *NETSCK, *OBJMGT, *OFCSRVR, *OPTICAL, *PGMADP, *PGMFAIL, *PRTDDTA, *PTFOBJ, *PTFOPR, *SAVRST, *SEC CFG, *SEC DIRSRVR, *SECIPC, *SECNAS, *SEC RUN, *SEC SCKD, *SECURITY, *SEC VFY, *SEC VLDL, *SERVICE, *SPLFDDTA, *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

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

```
Display System Value
System value . . . . . : QAUDLVL
Description . . . . . : Security auditing level

Auditing options
*AUDLVL2

Auditing options
```

# System Values

WRKSYSVAL QAUDLVL2

```
Display System
System value . . . . . : QAUDLVL2
Description . . . . . : Security auditing

Auditing
options
*ATNEVT
*AUTFAIL
*CREATE
*DELETE
*JOBDTA
*NETCMN
*NETSCK
*NETTELSVR
*NETUDP
*OBJMGT
*OFCSRV

Press Enter to continue.

F3=Exit  F12=Cancel
```

```
Display System Value
Display System Value - Help
- All security-related functions are audited.
  o Security configuration (See *SECCFG)
  o Changes or updates when doing directory service functions
    (See *SECDIRSRV)
  o Changes to interprocess communications (See *SECIPC)
  o Network authentication service actions (See *SECNAS)
  o Security run time functions (See *SECRUN)
  o Socket descriptor (See *SECCKD)
  o Use of verification functions (See *SECVFY)
  o Changes to validation list objects (See *SECVLDL)

Note: *SECURITY is composed of several values to allow you to
better customize your auditing. If you specify all of the
values, you will get the same auditing as if you specified
*SECURITY. The following values make up *SECURITY.

More...
F3=Exit help  F10=Move to top  F12=Cancel  F13=Information Assistant
F14=Print help
```

```
*SA...
*SECURITY
*SERVICE
*SPLFDTA
*SYSMGT
```

# 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*

```
Change System Value
System value . . . . . : QAUDCTL
Description . . . . . : Auditing control
Type choices, press Enter.
Auditing
control
*AUDLVL
*DBJAUD
*NOQTEMP
_____
_____
```

*CHGSECAUD – What is this?*

# System Values - Policy

## Define 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 Category System Value Description Alt. Expected Value Current Value Compl
Value Value Sts 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 205 200 *FAIL
_ QADLACTJ *
_ QADLSPLA * System Value ....: QACTJOB Compliance Status: *FAIL Category: *ALC
_ QADLTOTJ * Description . . .: Initial number of active jobs
_ QALWJOBITP * Shipped Value ...: 200
_ QALWBJRST * TG Recommend . . .: 200
_ QALWUSRDMN * Current Value ...: 200
_ QASTLVL *
_ QATNPGM * Compliance Cond ..: = _____ (INFO,=,LIKE,NLIKE,<>,<,>,<=,>=) Alert Status: *NO (*YES,*NO)
_ QAUDCTL * Expected Value(*NA/*SHIPPED/*TG/Value):
F1=Help F3=Exit Number of jobs . . . . . 205 1-32767
F14=Baseline to T
  
```

# 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
QASTIMI	*SYSCTL	User assistance level	*PASS	*INTERMED

# System Values - Policy

Enforce compliance against System Values policy

TGSYSCMP ARPT(\*YES) OUTPUT(\*HTML) ENFO(\*YES) RUNI(\*YES)

```
TG System Value Compliance (TGSYSCMP)
Type choices, press Enter.
Audit report . . . . . > *YES          *YES, *NO
Report output type . . . . . > *HTML      *, *PRINT, *OUTFILE, *HTML...
Enforcement . . . . . > *YES          *YES, *NO
Run interactively? . . . . . > *YES      *YES, *NO
```

# 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
-	QALWBJRST	*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

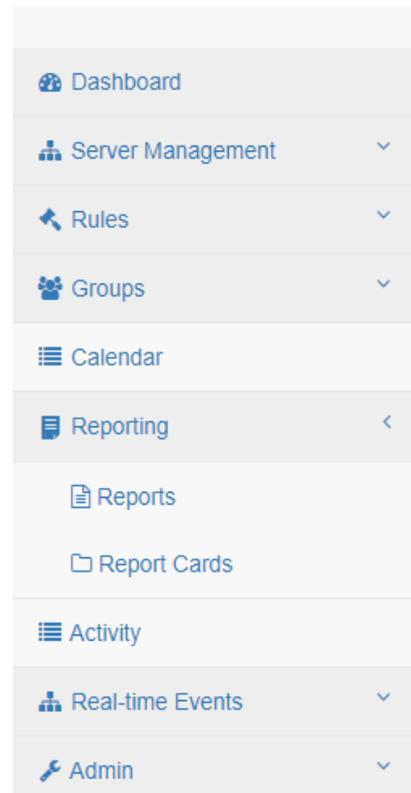
Privileged Users (common to most)

Special authorities

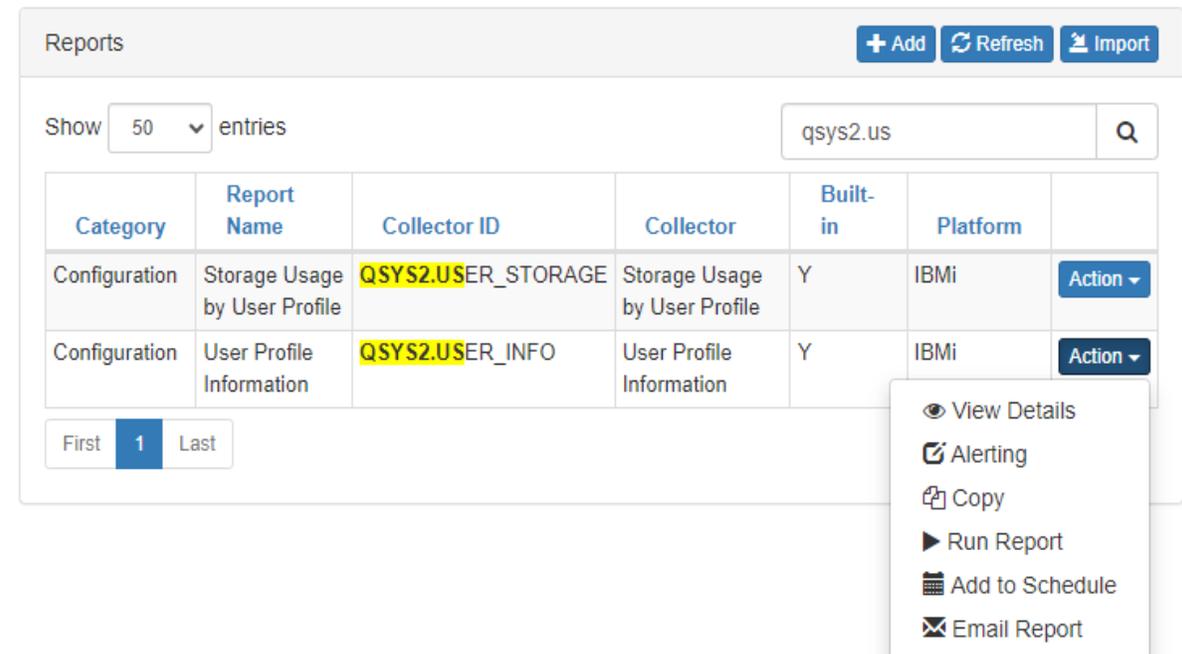
Group profiles

Limited capability

QSYS2.USER\_INFO



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



Reports

+ Add Refresh Import

Show 50 entries

qsys2.us

Category	Report Name	Collector ID	Collector	Built-in	Platform	
Configuration	Storage Usage by User Profile	QSYS2.USER_STORAGE	Storage Usage by User Profile	Y	IBMi	Action
Configuration	User Profile Information	QSYS2.USER_INFO	User Profile Information	Y	IBMi	Action

First 1 Last

- View Details
- Alerting
- Copy
- Run Report
- Add to Schedule
- Email Report

# User Profiles

New Report 2/4 | User Profile Information | ahUserInfo

**Report Fields** > >> << <

A list of the job attributes that are taken from the user's locale path.	User profile name.
A list of the options for users to customize their environment. Up to 7 options are returned.	The date and time the user last signed on
Country or region ID.	The number of sign-on attempts that were not valid since the last successful sign-on.
Date when the days used count was last reset to zero. The time portion of timestamp will always be 0.	The status of the user profile.
How the messages are delivered to the message queue used by the user.	The date the user's password was last changed.
	Indicates whether *NONE is specified for the password in the user profile.

Cancel Previous Next

# User Profiles

Reports + Add Refresh Import

Show  entries

Category	Report Name	Collector ID	Collector	Built-in	Platform	
Configuration	ahUserInfo	QSYS2.USER_INFO	User Profile Information	N	IBMi	Action ▾
Configuration	ah Function Usage Identifiers	QSYS2.FUNCTION_INFO	Function usage identifiers	N		View Details Edit Alerting Copy Run Report Add to Schedule Export Email Report
Resource	ah_dspusrprf	Database_Auditing	Database Changes	N		
Best Practices	Audit SGID executables	file	File	Y		
Best Practices	Audit SUID executables	file	File	Y		
Best Practices	Disable Automounting	processes	Processes	Y		
Best Practices	Ensure AIDE is installed	rpm_packages	Rpm Packages	Y		
Best Practices	Ensure AppArmor is not disabled in bootloader configuration	augeas	Augeas	Y		
Best Practices	Ensure Avahi Server is not enabled	file	File	Y		Action ▾
Best Practices	Ensure CUPS is not enabled	file	File	Y	Linux	Action ▾

# User Profiles

```
TG - Run Report (TGRPT)

Type choices, press Enter.

Collector ID . . . . . > QSYS2.USER_INFO
Collector Name . . . . . 'User Profile Information'
Report ID . . . . . > QSYS2_USER_INFO
Override report defaults? . . . . . *NO          *YES, *NO
Reload collector data . . . . . *YES          *AI, *YES, *NO
Report output type . . . . . > *HTML          *, *PRINT, *OUTFILE, *HTML...
Run interactively? . . . . . > *YES          *YES, *NO
```

# 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

```
TGTS1                                     Profile Inactivity Settings
ALAN

Inactivity until User Profile is disabled:  90           (Days)
Inactivity until User Profile is deleted : 180           (Days)
Delete profiles with password of *NONE . : *NO           (*YES/*NO)
Object owner for objects owned by deleted profiles. : QDFTOWN
Remove Deleted Profiles from TG User Group. . . . . : *NO           (*YES/*NO)
Remove Deleted Profiles from TG Rules . . . . . : *NO           (*YES/*NO)
Alert when Inactivity Found . . . . . : *NO           (*YES/*NO)

F1=Help  F3=Exit  F5=Refresh  F12=Cancel  F22=Run Inactivity Report  F23=Run Inactivity Enforcement
```

# User Profiles

```
TG Blueprint/Inactivity Compli (TGPRFCMP)

Type choices, press Enter.

Component . . . . . > *INACTIVITY
Audit report . . . . . > *YES          *YES, *NO
Users . . . . . *ALL          NAME, GENERIC*, *ALL
Days for disable user profile . . *DFT          *DFT, 0001-9999
Days for delete user profile . . *DFT          *DFT, 0001-9999
Report output type . . . . . *HTML        *, *PRINT, *OUTFILE, *HTML...
```

# User Profiles

Display Report

Report width . . . . . : 538  
Shift to column . . . . .

Line	Blueprint Id	User Name	Violation Category	Violation Keyword	Violation Description	Curr 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		ARTURQL	*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...
```

# 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.

# User Profiles – Privileged Access Management

## 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

```

TGTS1                               Blueprint - Add (Step 3/6)
ALAN                               User Profile Object Authority
Blueprint ID. . . . . : APP01_STATUS_CHANGE      Description. . . . . : APP01 STATUS CHANGE
Enter the Object Authority settings.

*USRPRF Object
Object Owner . . . . . : *DFT                    (*DFT,Name,*USRPRF)
Owner Authority . . . . . :                      (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . :                    (*AUTL,*USE,*CHANGE,*ALL,*EXCL

*MSGQ Object
Object Owner . . . . . : *DFT                    (*DFT,Name,*USRPRF)
Owner Authority . . . . . :                      (*CHANGE,*USE,*EXCLUDE,*ALL)
*PUBLIC Authority . . . . . :                    (*AUTL,*USE,*CHANGE,*ALL)
    
```

```

TGTS1                               Blueprint - Add (Step 4/6)
ALAN                               Authority List Settings
Blueprint ID . . . . . : APP01_STATUS_CHANGE
Description. . . . . : APP01 STATUS CHANGE

Set the Authority Lists.

4=Delete

      Authority  Authority
Opt  List       Value    Description
    
```

```

TGTS1                               Blueprint - Add (Step 5/6)
ALAN                               3rd party Integration
Blueprint ID . . . . . : APP01_STATUS_CHANGE
Description. . . . . : APP01 STATUS CHANGE

Set 3rd Party script to run and Pass User Profile($USRPRF) and/or Description ($TEXT)

4=Delete

      Script  Script
Opt  Type    Statement
    
```

```

TGTS1                               Blueprint - Add (Step 6/6)
ALAN                               Blueprint Permissions
Blueprint ID. . . . . : APP01_STATUS_CHANGE      Description. . . . . : APP01 STATUS CHANGE

Authorize admin/help desk users to use the blueprints.

User/Group. . . . . : ALANNONSEC (:TGUSGRP) +
Create Permissions. . . . . : *NO              (*YES,*NO)
Change Permissions. . . . . : *YES            (*YES,*NO)
    
```

# 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

IBM Navigator for i

Search 172.17.172.240 ALAN

### Exit Programs

View SQL

Actions

Exit Point Name	Exit Point Format	Registered	Complete	Exit Program Number	Exit Program Library	Exit Program
QIBM_QNPS_ENTRY	ENTR0100	YES	YES	1	TGPROD	NTW70002P
QIBM_QNPS_SPLF	SPLF0100	YES	YES	1	TGPROD	NTW70002P
QIBM_QPWFS_FILE_SERV	PWFS0100	YES	YES	1	TGPROD	NTW70002P
QIBM_QSO_ACCEPT	ACPT0100	YES	YES	1	TGPROD	NTW70001P
QIBM_QTG_DEVINIT	INIT0100	YES	YES	1	TGPROD	NTW70004P
QIBM_QTMF_CLIENT_REQ	VLRQ0100	YES	YES	1	TGPROD	NTW70003P
QIBM_QTMF_SERVER_REQ	VLRQ0100	YES	YES	1	TGPROD	NTW70003P
QIBM_QTMF_SVR_LOGON	TCPL0300	YES	YES	1	TGPROD	NTW70003P
QIBM_QTMX_SERVER_REQ	VLRQ0100	YES	YES	1	TGPROD	NTW70003P
QIBM_QTMX_SVR_LOGON	TCPL0300	YES	YES	1	TGPROD	NTW70003P
QIBM_QTOD_SERVER_REQ	VLRQ0100	YES	YES	1	TGPROD	NTW70003P
QIBM_QZDA_INIT	ZDAI0100	YES	YES	1	TGPROD	NTW70002P
QIBM_QZDA_NDB1	ZDAD0100	YES	YES	1	TGPROD	NTW70002P
QIBM_QZDA_NDB1	ZDAD0200	YES	YES	1	TGPROD	NTW70002P

Filtered Rows: 29 | Total Rows: 121

# 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

```
TGTS1                               Default Authority Schema - Add
ALAN
Schema ID . . . . . : APP01 IFS      (Name)
Schema Description. . . . . : Application 01 IFS Example
Alert Status. . . . . : *NO         (*YES,*NO)
Include IFS or Library Object.: *IFS   (*SYS,*IFS,*ALL,*NO)  IFS Depth: 99
Filter Details . . . . . : *NONE     (*NONE,Filter Name)      +
Object Scope
Object Name . . . . . : *NONE       (*NONE,*ALL,:TGGRP,Name,Generic*) +
Object Library. . . . . :           (*ALL,Name,Generic*)
```

```
TGTS1                               Default Authority Schema - Add
ALAN
Schema ID . . . . . : APP01 IFS      (Name)
Schema Description. . . . . : Application 01 IFS Example
Alert Status. . . . . : *NO         (*YES,*NO)
IFS Scope
IFS Path . . . . . : /demo/app01
Scope Authorities
Object Owner . . . . . : APP01      (*SAME,Name)
Authorization List. . . . . : *NONE  (*NONE,*SAME,Name)
Object Primary Group. . . . . : *NONE (*NONE,*SAME,Name)
*PUBLIC Object Authority. . . . . : *NONE (*ALL,*NONE,*OBJEXIST,
*PUBLIC Data Authority. . . . . : *EXCLUDE (*NONE,*RWX,*RX,*RW,*W
```

```
TGTS1                               Au
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log
IFS Authority Settings
Object Owner . . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
User Authority Settings
User Name. . . . . : *PUBLIC
Object Authority . . : *NONE
Data Authority . . . : *EXCLUDE
-----Object-----
Mat Exist Alter Ref
```

```
TGTS1                               Au
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log
IFS Authority Settings
Object Owner . . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
User Authority Settings
User Name. . . . . : APP01
Object Authority . . : *ALL
Data Authority . . . : *RWX
-----Object-----
```

```
TGTS1                               Au
ALAN
Schema ID . . . . . : APP01_IFS2
Schema Description . : Application 01 IFS Example
File System. . . . . : *IFS
IFS Scope
IFS Path . . . . . : /demo/app01/log
IFS Authority Settings
Object Owner . . . . . : APP01
Authorization List . : *NONE
Object Primary Group.: *NONE
User Authority Settings
User Name. . . . . : GRPPGMRS
Object Authority . . : *NONE
Data Authority . . . : *RX
-----Object-----
```

# Actions to Review from the Audit Journal

Reports + Add Refresh Import

Show  entries

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

# 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
```

# 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	IBMi	<ul style="list-style-type: none"> <li> View Details</li> <li> Alerting</li> <li> Copy</li> <li> Run Report</li> <li> Add to Schedule</li> <li> Email Report</li> </ul>
Configuration	Group PTFs Information	QSYS2.GROUP_PTF_INFO	Group PTFs Information	Y	IBMi	Action ▾
Configuration	Journal and Remote Journal Information	QSYS2.JOURNAL_INFO	Journal and Remote Journal Information	Y	IBMi	Action ▾
Resource	Journaled Objects	QSYS2.JOURNALED_OBJECTS	Journaled Objects	Y	IBMi	Action ▾
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 ▾

#	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

**Actions to review from the Audit Journal – Report Cards**

# 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

# Evidence - Supporting Documentation - Reporting

```

Subset Criteria - Rule ID . . . . . : *ALL           Rule Name . : *ALL           Calendar . . : *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
  
```

Opt	Rule ID	Rule Name	Calendar	Daily Count	Monthly Count	Yearly 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

# 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 File	Message Library	Description	Omit Select	Field Compare?	Reply
—	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

---

```
Rule ID/Name .: Qsecofr_Signon Monitor QSECOFR Signon
Message ID/Des: CPF1124 Job &3/&2/&1 started on &18 at &19 in subsystem &8 in &9. Job entered system on &20 at &21.&17
_____
_____
Please input criteria to filter report data and press Enter.
4=Delete

Opt      AND/OR      Nest      Field name      Operator      Value (quotes are not needed)      Nest
  _      _          Str          &2              =              QSECOFR              End
```

# Evidence - Supporting Documentation - Reporting

---

```
Rule ID. . . . . : Qsecofr_Signon
Rule Name. . . . . : Monitor QSECOFR Signon
```

```
2=Change 4=Delete 5=Display
```

Opt	Alt	Alert	Alert	Message to send	- Alert Criteria -	
	Seq	Type	Details		# Events	Freq
_	10	*MSG	ALAN	*MSG	*ANY	*ANY

# Evidence - Supporting Documentation - Reporting

---

```
Rule Name. . . . . : Qsecofr_Signon
Rule Description . . . . . : Monitor QSECOFR Signon

Alert Type. . . . . : _____ (*EMAIL, *MSG, *CMD, *SNMP, *SYSLOG, *EMAILDST, *TGCENTRAL)
Alert Sequence . . . . . : 20 (01-9999)

Alert Frequency:
Number of events . . . . . : *ANY (*ANY, 1-999999)
Event Frequency . . . . . : *ANY (*ANY, 1-999999)
Event. . . . . : _____ (DAY/HRS/MIN/SEC)
```

# Evidence - Supporting Documentation - Reporting

```
ALAN
Rule Name. . . . . : Qsecofr_Signon
Rule Description . . . . . : Monitor QSECOFR Signon
Alert Type. . . . . : *SYSLOG (*EMAI
Alert Sequence . . . . . : 20 (01-99
Alert Message. . . . . : *MSG
Syslog Provider Name. . . . . : ██████████
Alert Frequency:
Number of events . . . . . : *ANY (*ANY,
Event Frequency . . . . . : *ANY (*ANY,
Event. . . . . : (DAY/H
```

Sel	Syslog Provider
(1)	
—	ALAN
—	GRAYLOG
—	SIEM_ELK_GELF
—	SIEM_ELK_SYSLOG_TCP
—	SIEM_ELK_SYSLOG_UDP
—	SIEM_SYSLOG_SSL_TLS
—	SIEM_SYSLOG_TCP
—	SYSLOG_BASIC
—	SYSLOG_TCP_CEF

# Evidence - Supporting Documentation - Reporting

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

Alerts									
<a href="#">Email Config</a> <a href="#">Reset Filter</a> <a href="#">Filter</a> <a href="#">Refresh(48)</a>									
Show <input type="text" value="50"/> entries									
<input type="text" value="Search"/> <input type="button" value="Q"/>									
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?**

# FRESCHÉ 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](mailto:alan.hamm@freschesolutions.com)

[info@freschesolutions.com](mailto:info@freschesolutions.com)