



# Top 5 IBM i Security Vulnerabilities

---



**Carol Woodbury**  
CTO, DXR Security



**Pauline Brazil Ayala**  
VP, Compliance & Security Solutions

# Top Five IBM i Security Vulnerabilities

Carol Woodbury, CISSP, CRISC



carol@dxrsecurity.com



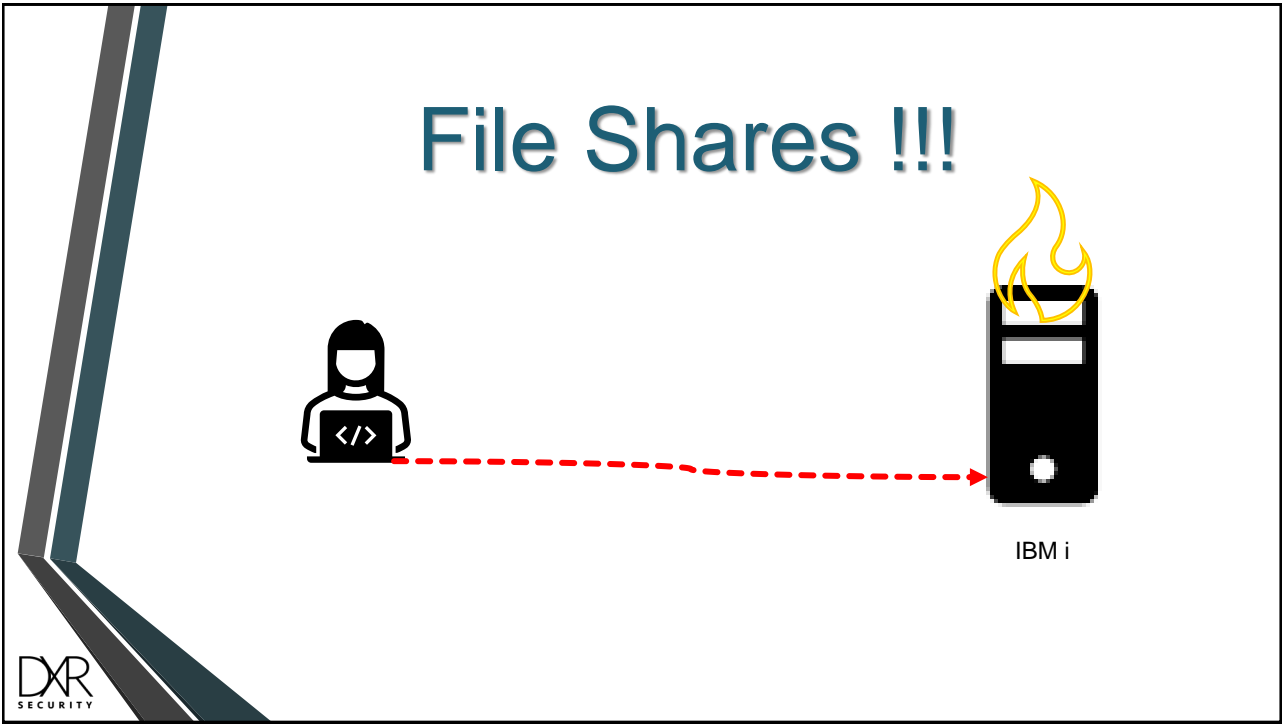
© DXRSecurity, All Rights Reserved.

1

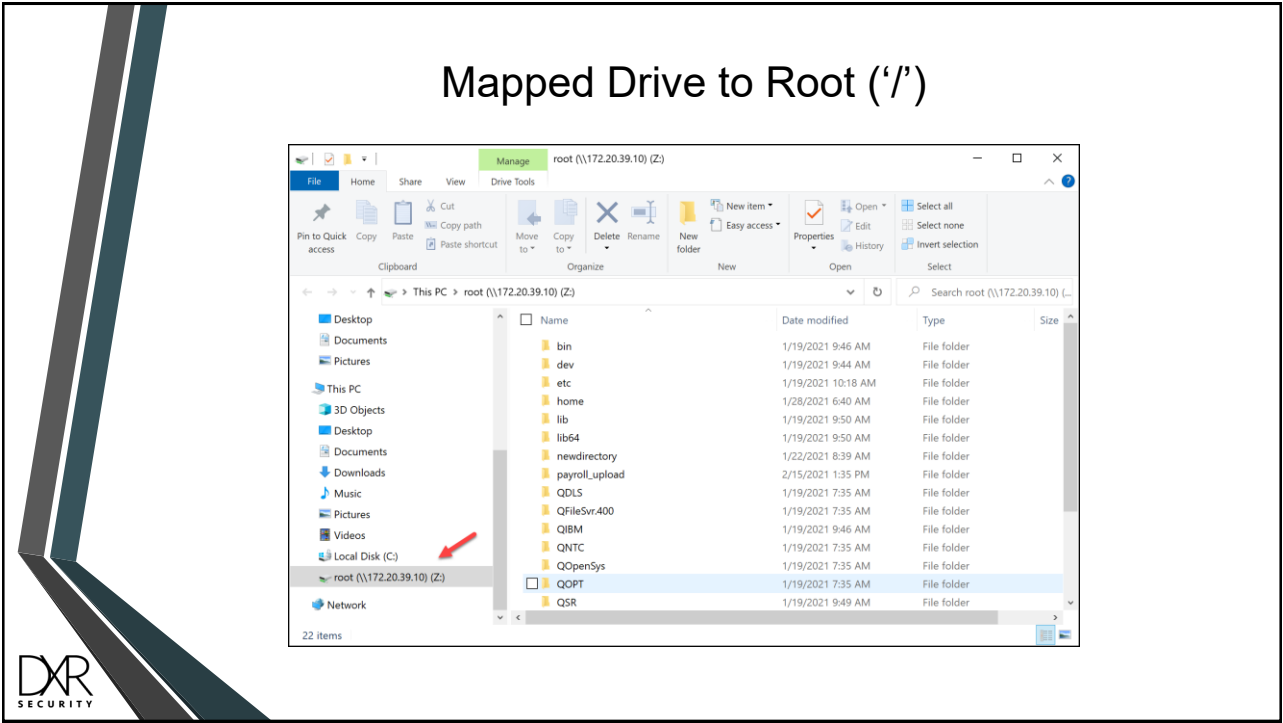
## Issue #1: Sharing Root ('/')



2



3



4

## Who Can Use a File Share?

- Until IBM i 7.5, there is no way to secure the share itself
- What the malware can do will depend on
  - How the share is defined – Read only or Read/Write
  - The user’s authority to the directory and objects in the directory
- ▪ Goals:
  - Reduce number and type of shares – fewer shares = lower risk
  - Secure access to objects shared to allow access only by users with a job responsibility to do so



5

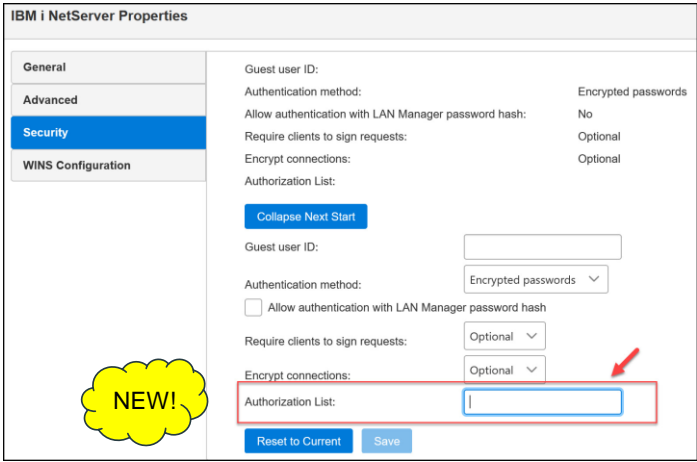
## Share Permissions

| Share Permission | What can be Accomplished  |
|------------------|---|
| Read share       | If user has at least *READ authority, contents can be read<br>Contents cannot be updated regardless of user’s authority to the object   |
| Read/Write share | If user has at least *READ authority, contents can be read<br>If user has at least *W (write) authority, contents can be modified<br>User must have sufficient authority for the operation being attempted (either a read or a write) |



6

## Controlling Access to NetServer with an Authorization List



IBM i NetServer Properties

General

Advanced

**Security**

WINS Configuration

Guest user ID:

Authentication method: Encrypted passwords

Allow authentication with LAN Manager password hash: No

Require clients to sign requests: Optional

Encrypt connections: Optional

Authorization List:

**NEW!**

Guest user ID:

Authentication method: Encrypted passwords

☐ Allow authentication with LAN Manager password hash

Require clients to sign requests: Optional

Encrypt connections: Optional

Authorization List:

Reset to Current Save

Suggested approach:

- Set \*PUBLIC to \*EXCLUDE
- Only authorize users who have a business need to map a drive

Remember:

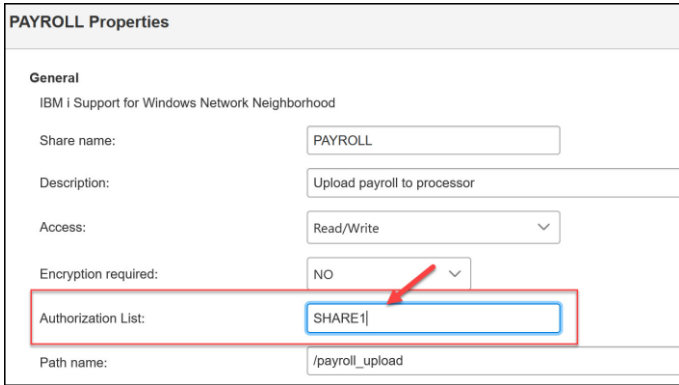
\*ALLOBJ provides access!!!

Authorization list secures no objects – Make name and description meaningful!



7

## Secure Individual Shares with an Authorization List



PAYROLL Properties

General

IBM i Support for Windows Network Neighborhood

Share name: PAYROLL

Description: Upload payroll to processor

Access: Read/Write

Encryption required: NO

**NEW!**

Authorization List: SHARE1

Path name: /payroll\_upload

Unlike share for NetServer, authority granted has meaning!!!

- \*USE to autl restricts access to Read-only
- \*CHANGE or greater (or \*ALLOBJ) grants Read/Write
- Authorities to underlying shared objects still apply

Make authorization list name and description meaningful as it secures no objects

➡ QSYS2.SERVER\_SHARE\_INFO enhanced to include name of authorization list



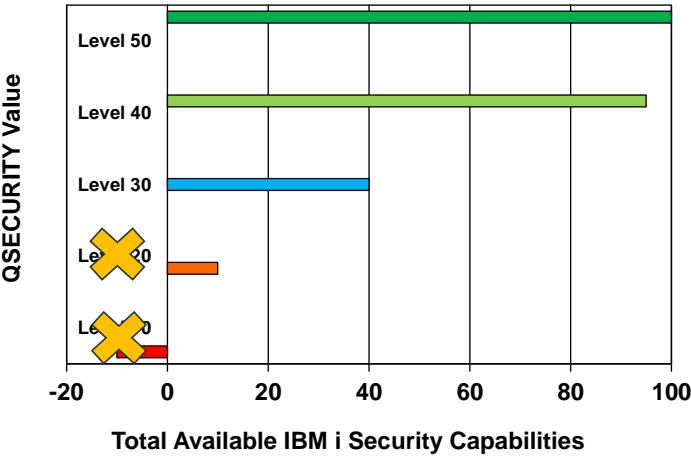
8

# Issue #2: Running at the Wrong QSECURITY Level



9

## Security Level (QSECURITY) – IBM i 7.5



10

## QSECURITY level 20 – IBM i 7.5

NEW!

- Can no longer specify 20 as a valid value for QSECURITY
- Systems currently at 20 will remain at 20 after upgrading.
- Systems being restored from media set to QSECURITY 20 will be set to whatever the system was prior to the restore
  - For example, if the system is set to 40 prior to the restore, the system will remain at 40 ... not 20.



11

## Moving to QSECURITY 40 from 30

- Add \*PGMFAIL and \*AUTFAIL to QAUDLVL system value
- Audit for AF entries subtypes B, C, D, R, S and J
- You do not care about AF – A (authority failures) when moving to security level 40. The same algorithm runs at level 40 that runs at all other levels



12



# Using the SQL Audit Journal Entry AF Table Function

```
1 SELECT entry_timestamp,
2        user_name,
3        qualified_job_name,
4        program_library,
5        program_name,
6        violation_type,
7        violation_type_detail,
8        object_library,
9        object_name,
10       object_type,
11       program_instruction
12 FROM TABLE (
13     systools.audit_journal_af(
14         starting_timestamp => current_timestamp - 7 days))
15 WHERE violation_type IN ('B', 'D', 'J', 'R', 'S');
```

| ENTRY_TIMESTAMP            | USER_NAME | QUALIFIED_JOB_NAME          | PROGRAM_LIBRARY | PROGRAM_NAME | VIOLATION_TYPE | VIOLATION_TYPE_DETAIL                               |
|----------------------------|-----------|-----------------------------|-----------------|--------------|----------------|---|
| 2022-05-31 15:41:55.323552 | CWOODBURY | 286537/CWOODBURY/QPADEV000F | QSYS ...        | QCMD ...     | D              | Use of unsupported interface, object domain failure |

- No need to run CPYAUDJRNE
- WHERE clauses get me to the right entries immediately
- TIMESTAMP arithmetic!!!



# Audit Journal Table Functions

- AF – Authority Failure (SYSTOOLS.AUDIT\_JOURNAL\_AF)
- CA – Changes to Authority (SYSTOOLS.AUDIT\_JOURNAL\_CA)
- OW – Ownership Changes (SYSTOOLS.AUDIT\_JOURNAL\_OW)
- PW – Password (SYSTOOLS.AUDIT\_JOURNAL\_PW)
- CO – Creation of objects (SYSTOOLS.AUDIT\_JOURNAL\_CO)
- CD – Command string (SYSTOOLS.AUDIT\_JOURNAL\_CD)
- CP – Creates and Changes to user profiles (SYSTOOLS.AUDIT\_JOURNAL\_CP)
- DO – Deletion of objects (SYSTOOLS.AUDIT\_JOURNAL\_DO)
- EV – Environment variable (SYSTOOLS.AUDIT\_JOURNAL\_EV)
- GR – Generic record (SYSTOOLS.AUDIT\_JOURNAL\_GR)
- SV – Changes to system values (SYSTOOLS.AUDIT\_JOURNAL\_SV)
- JS – Job start
- ST – Use of Service tools
- OM – Object management
- And they keep coming ...
  - <https://www.ibm.com/docs/en/i/7.5?topic=services-audit-journal-entry>



## Moving to QSECURITY 40 from 20

- \*ALLOBJ will be removed from all users not in \*SECOFR user class.
  - Need to determine where authority will come from since it will no longer – by default – come from \*ALLOBJ
  - Need to make sure users that should have \*ALLOBJ are either in the \*SECOFR user class or you modify the profile after IPLing to the higher level.
- Plus everything from previous slide
- Same authority checking algorithm so can test at level 20 prior to moving to level 40



15

## Issue #3: Running at Password Level 10 or 20



16

| System value |  |
|--------------|--|
| 0            | <p>Default</p> <p>Character set: A-Z, 0-9, \$, @, # and _</p> <p>Maximum length: 10</p>  |
| 1            | <p>Same as level 0 but gets rid of old NetServer password-<br/> <b>Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference</b></p>   |
| 2            | <p>Character set: Upper / lower case, all punctuation and special characters, numbers and spaces</p> <p>Maximum length: 128</p> <p>Keeps NetServer password, encrypts with old and new algorithms</p> <p>Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed</p> |
| 3            | <p>Same as level 2, gets rid of old encrypted password and old NetServer password<br/> <b>Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference</b></p>  |

At level 2, can sign on with a password that's ALL CAPS or all lower until password is changed. \*\*\* User education required!\*\*\*



**NEW!**

| System value |  |
|--------------|--|
| 0 / 1        | <p>Default</p> <p>Character set: A-Z, 0-9, \$, @, # and _</p> <p>Maximum length: 10</p> <p>LanMan password not stored at ANY level</p>   |
| 2            | <p>Character set: Upper / lower case, all punctuation and special characters, numbers and spaces</p> <p>Maximum length: 128</p> <p>Encrypts with old and new algorithms to accommodate both levels 0/1, 2/3 and 4</p> <p>Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed</p> |
| 3            | <p>Same as level 2, gets rid of old encrypted password</p> <p>Level 4 password generated and retained</p>  |
| 4            | <p><b>Stronger algorithm to store password hash. Only version stored is the one that works at level 4</b></p>  |



**NEW!**

| <b>Password hashes generated at QPWLVL 0/1</b>                                | <b>Password hashes generated at QPWLVL 2</b>   | <b>Password hashes generated at QPWLVL 3</b>   | <b>Password hash generated at QPWLVL 4</b> |
|---|--|--|--|
| All uppercase<br>All lowercase  | > Password no longer folded for authentication   | Used for authentication:<br>Mixed case – Level 2/3   | Level 4 version only                       |
| Regardless of what the user types (Carol) the password is folded: CAROL carol | Used for authentication:<br>Mixed case – Level 2/3<br><br>Hashes generated when password is changed:<br>- Mixed case – Level 2/3<br>- All uppercase<br>- All lowercase<br>- Mixed case – Level 4 | Hashes generated when password is changed:<br>- Mixed case – Level 2/3<br>- Mixed case - Level 4 |  |

All changes require an IPL




19

- Connection = anything *connecting to IBM i* where you've defined an IBM i user profile to make the connection and the password is hard-coded.
  - Profiles are often called "Service Accounts"
- Example:
  - ODBC / JDBC (e.g., WebSphere connections, client/server applications, Windows server connections)
- FTP
  - User: SERVICE1
  - Pwd: K3ls#Y


If set at QPWDLVL 0 or 1, this hardcoded password will fail at QPWDLVL 2 or 3 because what's stored is all lower and all




20



# Issue #4: Un- or Mis-managed User Profiles





21



## User Profile – Issue 4a

Too.Much.Power.





22

## Special Authorities (Capabilities)

| Special Authority | Definition  |
|-------------------|---|
| *AUDIT            | Auditing configuration  |
| *IOSYSCFG         | Communications configuration and management, creation of file shares  |
| *JOBCTL           | Management of any job on the system   |
| *SAVSYS           | Ability to save and restore any object on the system – or the entire system regardless of authority to the object |
| *SECADM           | Create/Change/Delete user profiles  |
| *SERVICE          | Ability to use Service Tools  |
| *SPLCTL           | Access to every spooled file on the system regardless of authority to the outq                                    |
| *ALLOBJ           | Access (All authority) to EVERY object on the system!!!!  |

- Assign special authorities by 'role'. If the user doesn't need it to perform their job, they shouldn't have the special authority.
- Special authorities assigned to a group are inherited by all members.



23

## Special Authority Analysis

```
--
-- description: Special Authority analysis
--
select user_name, special_authorities, group_profile_name, supplemental_group_list, text_description
from QSYS2.USER_INFO
where SPECIAL_AUTHORITIES like '%*ALLOBJ%' or
      AUTHORIZATION_NAME in (select USER_PROFILE_NAME
                             from QSYS2.GROUP_PROFILE_ENTRIES
                             where GROUP_PROFILE_NAME in (select AUTHORIZATION_NAME
                                                            from QSYS2.USER_INFO
                                                            where SPECIAL_AUTHORITIES like '%*ALLOBJ%'))
order by AUTHORIZATION_NAME;
```

| USER_NAME | SPECIAL_AUTHORITIES                           | GROUP_PROFILE_NAME | SUPPLEMENTAL_GROUP_LIST | TEXT_DESCRIPTION                          |
|-----------|---|--------------------|-------------------------|---|
| WANGZBO   | *ALLOBJ *SECADM *JOBCTL *SPLCTL *SAV... *NONE |                    | <NULL>                  | Tim M Rowe - IBM Presentor extraordinaire |
| WASEXP001 | <NULL>  | EXPRESSGRP         | <NULL>                  | REQUIRED FOR EXPRES SERVER LAB            |
| WASEXP002 | <NULL>  | EXPRESSGRP         | <NULL>                  | REQUIRED FOR EXPRES SERVER LAB            |
| WASEXP003 | <NULL>  | EXPRESSGRP         | <NULL>                  | REQUIRED FOR EXPRES SERVER LAB            |
| WASEXP004 | <NULL>  | EXPRESSGRP         | <NULL>                  | REQUIRED FOR EXPRES SERVER LAB            |
| WASEXP005 | <NULL>  | EXPRESSGRP         | <NULL>                  | REQUIRED FOR EXPRES SERVER LAB            |

Done: 1,190 rows retrieved.



24

# User Profile – Issue 4b

Default passwords



25

# Default Passwords with SQL

```
--
-- description: User profiles with default passwords
--
select USER_NAME, STATUS, PASSWORD_EXPIRATION_INTERVAL, SPECIAL_AUTHORITIES,
       GROUP_PROFILE_NAME, SUPPLEMENTAL_GROUP_LIST, LAST_USED_TIMESTAMP,
       CREATION_TIMESTAMP, USER_CREATOR, TEXT_DESCRIPTION
from qsys2.user_info
where USER_DEFAULT_PASSWORD = 'YES'
order by status;
```

| USER_NAME          | STATUS    | PASSWORD_EXPIRATION_INTERVAL | SPECIAL_AUTHORITIES     | GROUP_PROFILE_NAME | SUPPLEMENTAL_GROUP_LIST | LAST_USED_TIMESTAMP   |
|--------------------|-----------|------------------------------|-------------------------|--------------------|-------------------------|-----------------------|
| Authorization Name | Status    | Password Expiration Interval |                         | Group Profile Name | Supplemental Group List | Last Used Timestamp   |
| IOAT               | *DISABLED | 0                            | <NULL>                  | *NONE              | <NULL>                  | <NULL>                |
| RED                | *DISABLED | 0                            | <NULL>                  | MYGROUP            | <NULL>                  | <NULL>                |
| YSQL               | *DISABLED | 0                            | <NULL>                  | *NONE              | <NULL>                  | 2022-05-12 00:00:00.0 |
| YIUSR03            | *DISABLED | 0                            | <NULL>                  | *NONE              | <NULL>                  | <NULL>                |
| YLAB               | *DISABLED | 0                            | <NULL>                  | *NONE              | <NULL>                  | 2022-04-23 00:00:00.0 |
| SUPERUSER          | *DISABLED | 0                            | *ALLOBJ *SECADM *JOB... | *NONE              | <NULL>                  | 2022-05-15 00:00:00.0 |
| LAB01              | *DISABLED | -1                           | <NULL>                  | QPGMR              | <NULL>                  | 2021-02-11 00:00:00.0 |



26

Create User Profile (CRTUSRPRF) – 1 (New default in IBM i 7.5

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . .

newprofile

Name

User password . . . . .

\*NONE

Set password to expired . . . . .

\*yes

\*NO, \*YES

Status . . . . .

\*ENABLED

\*ENABLED, \*DISABLED

User class . . . . .

\*USER

\*USER, \*SYSOPR, \*PGMR...

Assistance level . . . . .

\*SYSVAL

\*SYSVAL, \*BASIC, \*INTERMED...

Current library . . . . .

\*CRTDFT

Name, \*CRTDFT

Initial program to call . . . . .

\*NONE

Name, \*NONE

Library . . . . .

Name, \*LIBL, \*CURLIB

Initial menu . . . . .

MAIN

Name, \*SIGNOFF

Library . . . . .

\*LIBL

Name, \*LIBL, \*CURLIB

Limit capabilities . . . . .

\*NO

\*NO, \*PARTIAL, \*YES

Text 'description' . . . . .

Make this meaningful!!!

F3=Exit

F4=Prompt

F5=Refresh

F10=Additional parameters

F12=Cancel

Bottom

F13=How to use this display

F24=More keys

NEW!

- IBM i 7.5 changes:
- Password now defaults to \*NONE (rather than \*USRPRF)
  - Can now specify password expired \*YES with password \*NONE

27

QPWDRULES

- \*PWDSYSVAL or
- \*CHRLMTAJC
  - \*CHRLMTREP
  - \*DGTLMATAJC
  - \*DGTLMTFST
  - \*DGTMLTLST
  - \*DGTMAXn
  - \*DGTMINn
  - \*LMTSAMPOS
  - \*LMTPRFNAME
  - \*LTRLMTAJC
  - \*LTRLMTFST
  - \*LTRLMTLST
  - \*LTRMAXn
  - \*LTRMINn

- \*MAXLENnnn
- \*MINLENnnn
- \*MIXCASEnnn
- \*REQANY3
- \*SPCCHRLMTAJC
- \*SPCCHRLMTFST
- \*SPCCHRLMTLST
- \*SPCCHRMAXn
- \*SPCCHRMINn

V7R2

- \*ALLCRTCHG

➡ Recommended: Rules are all in one place, more options



## System Values – Password Composition Rules

General

Validation 1

Validation 2

Expiration

System Values: Password

Password level (current):  
Long passwords using an unlimited character set (3) \*

Password validation options (QPWDRULES):  

☐ Use the validation system values on the Validation 1 tab

☒ Use the following validation rules. Certain corresponding system values on the Validation 1 tab will be ignored.

Password Lengths:  

☐ Minimum length (1-128) (QPWDMINLEN): 1 1 - 128

☐ Maximum length (1-128) (QPWDMAXLEN): 128 1 - 128

Restrict repeating characters: Characters may be used more than once  

☐ Require a new character in each position from previous password

☒ Restrict user profile in password

☐ Require a minimum number of lowercase and uppercase letters (0-9): 0 0 - 9

☒ Require characters from at least 3 of the following types of characters (upper, lower, digit, special)

☒ Enforce all password validation options when creating or changing a password with CRTUSRPRF or CHGUSRPRF.

29

## User Profile – Issue 4c

A photograph of a simple wooden chair with a curved backrest, positioned on a polished wooden floor. The chair is empty, and the lighting is soft, creating a calm and somewhat somber atmosphere, which visually represents the concept of an 'inactive profile'.

Inactive profiles

30

© DXR Security, All Rights Reserved.

15

# Managing Inactive Profiles with an SQL

```
--
-- description: User profiles that haven't been used in the last 3 months
--
SELECT user_name,
       date(last_used_timestamp) as last_used,
       timestamp(previous_signon, 0) as last_signon,
       timestamp(creation_timestamp, 0) as create_time,
       status,
       text_description
FROM QSYS2.USER_INFO
WHERE (last_used_timestamp IS NULL
       OR last_used_timestamp < CURRENT_TIMESTAMP - 3 MONTHS)
       AND (creation_timestamp < CURRENT_TIMESTAMP - 3 MONTHS);
```

| USER_NAME  | LAST_USED  | LAST_SIGNON | CREATE_TIME         | STATUS   | TEXT_DESCRIPTION |
|------------|------------|-------------|---------------------|----------|------------------|
| FRANKDBA26 | <NULL>     | <NULL>      | 2019-11-06 04:40:09 | *ENABLED | <NULL>           |
| FRANKDBA27 | <NULL>     | <NULL>      | 2019-11-06 04:40:47 | *ENABLED | <NULL>           |
| FRANKDBA28 | <NULL>     | <NULL>      | 2019-11-06 04:40:35 | *ENABLED | <NULL>           |
| FRANKDBA99 | 11/06/2019 | <NULL>      | 2019-11-05 15:28:54 | *ENABLED | <NULL>           |

Done: 1,638 rows retrieved.

# QSYS2.user\_info – Inactive Profiles

File Edit View Run VisualExplain Monitor Options Connection Tools Help

4

5 SELECT authorization\_name,

6 last\_used\_timestamp,

7 previous\_signon,

8 creation\_timestamp,

9 status,

10 text\_description

11 FROM QSYS2.USER\_INFO

12 WHERE (last\_used\_timestamp IS NULL

13 OR last\_used\_timestamp < CURRENT\_TIMESTAMP - 3 MONTHS)

14 AND (creation\_timestamp < CURRENT\_TIMESTAMP - 3 MONTHS);

| Authorization Name | Last Used Timestamp | Previous Signon | Creation Timestamp | Status |
|--------------------|---------------------|-----------------|--------------------|--------|
| AUTHORIZATION_NAME | LAST_USED_TIMESTAMP | PREVIOUS_SIGNON | CREATION_TIMESTAMP | STATUS |

# SYSTOOLS.CHANGE\_USER\_PROFILE() table function

File Edit View Run Visual Explain Monitor Options Connection Tools Help

18 SELECT \* FROM QSYS2.USER\_INFO,

19       TABLE(SYSTOOLS.CHANGE\_USER\_PROFILE (

20                   P\_USER\_NAME => AUTHORIZATION\_NAME,

21                   P\_STATUS    => '\*DISABLED',

22                   PREVIEW     => 'NO'))

23 WHERE (last\_used\_timestamp is NULL or

24       last\_used\_timestamp < current\_timestamp - 3 months ) and

25       (creation\_timestamp < current\_timestamp - 3 months ) and

26       authorization\_name <> 'QSECOFR';

| Authorization Name | Previous Signon            | Sign On Attempts Not Valid  | Status       | Passw Change Date        |
|--------------------|----------------------------|-----------------------------|--------------|--------------------------|
| AUTHORIZATION_NAME | PREVIOUS_SIGNON            | SIGN_ON_ATTEMPTS_NOT_VAL ID | STATUS       | NETSERVER_DISABLED PASSW |
| JOHN               | 2021-01-27 09:09:36.000000 | 0                           | *DISABLED NO | 2021-0                   |

Changes the user profile!

Available in V7R3 TR10 and V7R4 TR4  
<https://www.ibm.com/docs/en/i/7.4?topic=services-change-user-profile-table-function>



# Issue #5: Too Much Access to Data



## Wide-open Access to Data



- No recognition that data has value
- Critical data has not been identified, much less secured
- QCRTAUT set to \*ALL
- Database files not secured
- IFS objects not secured
- Too many profiles with \*ALLOBJ



35

## Afraid of Breaking Something

- Use Authority Collection by user to determine what objects are accessed and authority required to successfully remove \*ALLOBJ
  - IBM i 7.3
- Use Authority Collection by object to determine which profiles are accessing an object (in a library, directory or folder) to successfully secure objects
  - IBM i 7.4
- Removes the guesswork! ←



36

## Data is an Asset and Needs to be Protected

- Don't have to secure ALL objects on the system!
- Identify critical data (whether in a library or IFS)
- Good security settings protect against purposeful loss as well as accidental errors



37

## Avoid Vulnerabilities: Implement Defense in Depth

- Multiple layers of defense:
  - Best practices for system values
    - Security level (QSECURITY)
    - Password level and composition rules (QPWDLVL and QPWDRULES)
  - Least privilege access assigned to User profiles
  - Deny by default object level authorities for both objects in libraries as well as directories
  - Exit programs for more granular access controls
  - Encryption additional control of who sees data (including the omission of \*ALLOBJ users) and potential separation of duties



38

## For More Information



### IBM i Security Reference – PDF

[https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_75/rzarl/sc415302.pdf?view=kc](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_75/rzarl/sc415302.pdf?view=kc)

### IBM i Services

- <https://www.ibm.com/support/pages/node/1119123>

### SQL Tutorials – Scott Forstie

- <https://ibm.biz/Db2foriSQLTutor>

### Memo to Users

- <https://www.ibm.com/docs/en/i/7.5?topic=documentation-memo-users>

IBM i Security Administration and Compliance, 3<sup>rd</sup> edition, by Carol Woodbury, 2020 available from Amazon.com and MCPressOnline Bookstore

Mastering IBM i Security by Carol Woodbury, 2022. Order here:

- <https://www.mc-store.com/products/mastering-ibm-i-security>

# Security Auditing

Dashboard

Server Management &lt;

Servers

Server Groups

Rules &gt;

Groups &gt;

Calendar

Reporting &lt;

Reports

Report Cards

Activity

Real-time Events &lt;

Network Activity

Detect Activity

Alert

Admin &lt;

## Reports

+ Add

Refresh

Import

Show 50 entries

Search



| Category      | Report Name   | Collector ID             | Collector                             | Built-in | Platform |          |
|---------------|---|--------------------------|---------------------------------------|----------|----------|----------|
| Resource      | Customer Master Data  | Database_Content         | Database Content                      | N        | IBMi     | Action > |
| Resource      | Customer Master DB Changes                                  | Database_Auditing        | Database Changes                      | N        | IBMi     | Action > |
| Configuration | Access Control List Changes                                 | Journal_VA               | Access Control List Changes           | Y        | IBMi     | Action > |
| Configuration | Actions that Affect a Job are Audited                       | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | Active Job Information                                      | QSYS2.ACTIVE_JOB_INFO    | Active job information                | Y        | IBMi     | Action > |
| Configuration | Adopting Authority from a Program Owner is Audited          | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | All Deletions of External Objects on the System are Audited | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | All Object Creations are Audited                            | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | All Optical Functions are Audited                           | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | All Security Functions are Audited                          | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | Alternate Subsystem Configurations                          | QSYS2.SERVER_SBS_ROUTING | Alternate Subsystem Configurations    | Y        | IBMi     | Action > |
| Configuration | Attention Events are Audited                                | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | Auditing End Action set to Power Down System                | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | Authority Changes to Restored Objects                       | Journal_RA               | Authority Changes to Restored Objects | Y        | IBMi     | Action > |
| Configuration | Authorization Failures are Audited                          | System_Values            | System Value Information              | Y        | IBMi     | Action > |
| Configuration | Certificate Details   | Keystore_Data            | Keystore Data                         | Y        | IBMi     | Action > |
| Configuration | Certificates Expired  | Keystore_Data            | Keystore Data                         | Y        | IBMi     | Action > |



Dashboard

Server Management

Servers

Server Groups

Rules

Groups

Calendar

Reporting

Reports

Report Cards

Activity

Real-time Events

Network Activity

Detect Activity

Alert

Admin

## Reports

+ Add

Refresh

Import

Show 50 entries

Journal

Q

| Category      | Report Name  | Collector ID       | Collector  | Built-in | Platform |        |
|---------------|--|--------------------|--|----------|----------|--------|
| Configuration | Access Control List Changes                                    | Journal_VA         | Access Control List Changes                                    | Y        | IBMi     | Action |
| Configuration | Authority Changes to Restored Objects                          | Journal_RA         | Authority Changes to Restored Objects                          | Y        | IBMi     | Action |
| Configuration | Change Request Descriptor Changes                              | Journal_CQ         | Change Request Descriptor Changes                              | Y        | IBMi     | Action |
| Configuration | Cryptographic Configuration Changes                            | Journal_CY         | Cryptographic Configuration Changes                            | Y        | IBMi     | Action |
| Configuration | EIM Attribute Changes  | Journal_AU         | EIM Attribute Changes  | Y        | IBMi     | Action |
| Configuration | Environment Variable Changes                                   | Journal_EV         | Environment Variable Changes                                   | Y        | IBMi     | Action |
| Configuration | Job Descriptions that Contain User Profile Names were Restored | Journal_RJ         | Job Descriptions that Contain User Profile Names were Restored | Y        | IBMi     | Action |
| Configuration | Journal Monitor Alerts   | Det_JrnMon_Alerts  | Journal Monitor Alerts   | Y        | IBMi     | Action |
| Configuration | Journal Monitor Rules  | Det_JrnMon_Rules   | Journal Monitor Rules  | Y        | IBMi     | Action |
| Configuration | Journal Monitor Rules for SIEM                                 | Det_Jrn_SIEM_Rules | Journal Monitor Rules for SIEM                                 | Y        | IBMi     | Action |
| Configuration | Journal and Remote Journal Information                         | QSYS2_JOURNAL_INFO | Journal and Remote Journal Information                         | Y        | IBMi     | Action |
| Configuration | Key Ring File Changes  | Journal_KF         | Key Ring File Changes  | Y        | IBMi     | Action |
| Configuration | Object Auditing Attribute Changes                              | Journal_AD         | Object Auditing Attribute Changes                              | Y        | IBMi     | Action |
| Configuration | Primary Group Changes for Restored Objects                     | Journal_RZ         | Primary Group Changes for Restored Objects                     | Y        | IBMi     | Action |
| Configuration | Program Changes to Adopt Owner Authority                       | Journal_PA         | Program Changes to Adopt Owner Authority                       | Y        | IBMi     | Action |
| Configuration | Programs Restored that Adopt Owner Authority                   | Journal_RP         | Programs Restored that Adopt Owner Authority                   | Y        | IBMi     | Action |
| Configuration | Programs that Adopt Authority were Executed                    | Journal_AP         | Programs that Adopt Authority were Executed                    | Y        | IBMi     | Action |

Dashboard

Server Management

Servers

Server Groups

Rules

Groups

Calendar

Reporting

Reports

Report Cards

Activity

Real-time Events

Network Activity

Detect Activity

Alert

Admin

## Reports

+ Add

Refresh

Import

Show 50 entries

sign



| Category | Report Name  | Collector ID                  | Collector                              | Built-in | Platform |        |
|----------|--|-------------------------------|--|----------|----------|--------|
| Network  | Asynchronous <b>Sign</b> als Processed                       | Journal_SG                    | Asynchronous <b>Sign</b> als Processed | Y        | IBMi     | Action |
| Network  | Remote <b>Sign</b> -on Control                               | System_Values                 | System Value Information               | Y        | IBMi     | Action |
| Network  | <b>Sign</b> on Server Transactions Report                    | Network_Trans_ <b>Sign</b> on | Network Transactions <b>Sign</b> on    | Y        | IBMi     | Action |
| Profile  | Disable Profile After Maximum Failed <b>Sign</b> on Attempts | System_Values                 | System Value Information               | Y        | IBMi     | Action |
| Profile  | Invalid <b>Sign</b> -on Attempts                             | Journal_PW                    | Invalid <b>Sign</b> -on Attempts       | Y        | IBMi     | Action |
| Resource | Maximum <b>sign</b> -on attempts allowed is NOMAX            | System_Values                 | System Value Information               | Y        |          |        |

First 1 Last

View Details

Alerting

Copy

Run Report

Add to Schedule

Email Report

Last

Run Now

sign

Q

Action ▼

Special date values make it easy to automate scheduling

Invalid Sign-on Attempts

Server Name

TGSE1.TRINITYGUARD.COM

From Date

\*LMS Last Month Start

\*CUR Current Date

\*CMS Current Month Start

\*LMS Last Month Start

\*LME Last Month End

\*LYS Last Year Start

\*LYE Last Year End

\*LDS Last Day Start

\*LWS Last Week Start

To Date

\*CUR Current Date

From

To Time

User Name

\*ALL

Cancel

Run Now

TRINITY GUARD

Invalid Sign-on Attempts For User: \*ALL From: 030123 00:00 To: 041823 23:59

TGSE1ADMIN2023-04-1803:25:52

Search...Q

| Timestamp of entry         | Name of job | Name of user | Number of job | Name of program | User profile | System name | Remote address | Length of specific data | P-Pwd, U-User name, A-APPC, D-DST user, E-DST Pwd | User profile name | Device name | Remote location name | Local location name | Network ID | Name of object | Library name | Object type | ASP name | ASP number |
|----------------------------|-------------|--------------|---------------|-----------------|--------------|-------------|----------------|-------------------------|---|-------------------|-------------|----------------------|---------------------|------------|----------------|--------------|-------------|----------|------------|
| 2023-03-06-11.17.46.459072 | QTFTP00037  | QTCP         | 322033        | QTMFSRVR        | QTCP         | TGSE1       | 10.11.12.34    | 118                     | P   | PMB               | *N          |                      |                     |            |                |              |             |          |            |
| 2023-03-09-16.59.22.022864 | QINTER      | QSYS         | 321965        | QLESPI          | QSYS         | TGSE1       | 10.11.12.33    | 118                     | P   | PMBTEST2          | QPADEV0006  |                      |                     |            |                |              |             |          |            |
| 2023-03-09-16.59.25.388336 | QINTER      | QSYS         | 321965        | QLESPI          | QSYS         | TGSE1       | 10.11.12.33    | 118                     | P   | PMBTEST2          | QPADEV0006  |                      |                     |            |                |              |             |          |            |
| 2023-03-21-09.28.30.277328 | QINTER      | QSYS         | 321965        | QLESPI          | QSYS         | TGSE1       | 10.11.12.39    | 118                     | P   | PMB               | QPADEV0001  |                      |                     |            |                |              |             |          |            |
| 2023-04-18-02.07.20.845808 | QINTER      | QSYS         | 321965        | QLESPI          | QSYS         | TGSE1       | 10.11.12.33    | 118                     | U   | PMBASIC           | QPADEV0002  |                      |                     |            |                |              |             |          |            |

Previous1Next

50 entries 1 to 50 / 5

Alert

Admin

Users

|          |                        |                |                  |             |           |        |
|----------|------------------------|----------------|------------------|-------------|-----------|--------|
| SCHEDULE | TGSE1.TRINITYGUARD.COM | Sarbanes-Oxley | 2023-02-28 14:48 | Report Card | Completed | Action |
| SCHEDULE | TGSE1.TRINITYGUARD.COM | Sarbanes-Oxley | 2023-02-28 14:44 | Report Card | Completed | Action |
| SCHEDULE | TGSE1.TRINITYGUARD.COM | Sarbanes-Oxley | 2023-02-28 14:41 | Report Card | Completed | Action |
| SCHEDULE | TGSE1.TRINITYGUARD.COM | Sarbanes-Oxley | 2023-02-28 14:38 | Report Card | Completed | Action |



## Invalid Sign-on Attempts - help

This report displays password validation failures. The data related to this report is retrieved from the system security audit journal (QAUDJRN). The journal entry type associated with this event is PW.

Types of entries:

- A** - APPC bind failure.
- C** - User authentication with the CHKPWD command failed.
- D** - Service tools user ID name not valid.
- E** - Service tools user ID password not valid.
- P** - Password not valid.
- Q** - Attempted sign-on (user authentication) failed because user profile is disabled.
- R** - Attempted sign-on (user authentication) failed because password was expired. This audit record might not occur for some user authentication mechanisms. Some authentication mechanisms do not check for expired passwords.
- S** - SQL Decryption password is not valid.
- U** - User name not valid.
- X** - Service tools user ID is disabled.
- Y** - Service tools user ID not valid.
- Z** - Service tools user ID password not valid.

PASS = PW Journal entries were not found in QAUDJRN.

FAIL = PW Journal entries were found in QAUDJRN.

For PW journal entries to be generated, the QAUDLVL system value must contain \*AUTFAIL.



## PCI DSS 4.0

TGSE1

ADMIN

2022-11-30

11:37:45

| Category      | Regulation | Report Name  | Number of Violations | Exceptions | Pass/Fail Status | Status    |
|---------------|------------|--|----------------------|------------|------------------|-----------|
| Profile       | 10.7.3.B   | <a href="#">Authority Failures</a>                     | 1861                 |            | Fail             | Completed |
| Network       | 11.4       | <a href="#">Intrusion Monitor Events</a>               | 0                    |            | Pass             | Completed |
| Profile       | 10.2.1.4   | <a href="#">Invalid Sign-on Attempts</a>               | 2                    |            | Fail             | Completed |
| Network       | 1.1.2      | <a href="#">Secure Socket Connections</a>              | 0                    |            | Pass             | Completed |
| Configuration | 10.6.3.B   | <a href="#">System Values Changes</a>                  | 694                  |            | Fail             | Completed |
| Resource      | 10.9       | <a href="#">Network Resource Accesses</a>              | 0                    |            | Pass             | Completed |
| Network       | 1.1.2      | <a href="#">Server Sessions Started or Ended</a>       | 0                    |            | Pass             | Completed |
| Profile       | 11.3.1.3   | <a href="#">Blueprint Non-Compliance User Profiles</a> | 21                   |            | Fail             | Completed |
| Configuration | 3.6        | <a href="#">Certificate Details</a>                    | 0                    |            | Pass             | Completed |
| Configuration | 12.10.5    | <a href="#">Command Monitor Rules</a>                  | 4                    |            | Fail             | Completed |
| Configuration | 12.10.5    | <a href="#">Journal Monitor Rules</a>                  | 10                   |            | Fail             | Completed |
| Configuration | 12.10.5    | <a href="#">Message Queue Rules</a>                    | 69                   |            | Fail             | Completed |
| Network       | 12.10.5    | <a href="#">SIEM Activity</a>                          | 0                    |            | Information Only | Completed |
| Profile       | 2.2.2      | <a href="#">Enabled IBM Profiles</a>                   | 52                   |            | Fail             | Completed |
| Network       | 1.5.1      | <a href="#">Exit Point Configuration Report</a>        | 29                   |            | Fail             | Completed |
| Network       | 11.5       | <a href="#">Exit Point Configuration Changes</a>       | 1                    |            | Fail             | Completed |
| Network       | 8.2.8      | <a href="#">ISL Configuration Settings</a>             | 1                    |            | Fail             | Completed |

SCHEDULE

TGSE1 TRINITYGUARD.COM

Sarbanes-Oxley

2023-01-18 01:00

Report Card

Completed



## TGFree Security Assessment

TGSE1

ADMIN

2023-02-28

14:22:06

| Category      | Regulation | Report Name   | Number of Violations | Exceptions | Pass/Fail Status | Status    |
|---------------|------------|---|----------------------|------------|------------------|-----------|
| Resource      |            | Authorization Lists with Public Access                      | 7                    |            | Fail             | Completed |
| Profile       |            | Group Profiles with Passwords                               | 1                    |            | Fail             | Completed |
| Resource      |            | Integrated File System Security                             | 0                    |            | Pass             | Completed |
| Network       |            | NetServer shares  | 4                    |            | Fail             | Completed |
| Network       |            | Network Connection Details                                  | 68                   |            | Information Only | Completed |
| Profile       |            | User Profiles Not Used in 90 Days                           | 22                   |            | Fail             | Completed |
| Profile       |            | Powerful User Profiles                                      | 18                   |            | Fail             | Completed |
| Profile       |            | User Profile = Password                                     | 18                   |            | Fail             | Completed |
| Resource      |            | Allow Object Restore Option                                 | 1                    |            | Fail             | Completed |
| Resource      |            | Allow User Domain Objects in Libraries                      | 1                    |            | Fail             | Completed |
| Configuration |            | System, User, and Object Auditing Control Configuration     | 0                    |            | Pass             | Completed |
| Configuration |            | Attention Events are Audited                                | 0                    |            | Fail             | Completed |
| Configuration |            | Authorization Failures are Audited                          | 1                    |            | Pass             | Completed |
| Configuration |            | All Object Creations are Audited                            | 1                    |            | Pass             | Completed |
| Configuration |            | All Deletions of External Objects on the System are Audited | 1                    |            | Pass             | Completed |
| Configuration |            | Actions that Affect a Job are Audited                       | 0                    |            | Fail             | Completed |
| Configuration |            | Networking and Communications Functions are Audited         | 0                    |            | Fail             | Completed |



## User Profile = Password For User: \*ALL



|       |       |            |          |
|-------|-------|------------|----------|
| TGSE1 | ADMIN | 2023-02-28 | 14:38:48 |
|-------|-------|------------|----------|

| User Profile Name | User class | Status   | Limited capability | Password change date: YYYYMMDD | Previous sign-on date: YYYYMMDD | Verifications not valid | Owner   | Group profile | Group authority | Text description         | Special authorities   |
|-------------------|------------|----------|--------------------|--------------------------------|---------------------------------|-------------------------|---------|---------------|-----------------|--------------------------|---|
| ARPPGMR           | *PGMR      | *ENABLED | *NO                | 190808                         | 190816                          | 0                       | *USRPRF | *NONE         | *NONE           |                          | *NONE   |
| ARP1              | *USER      | *ENABLED | *NO                | 180420                         | 181029                          | 0                       | *USRPRF | *NONE         | *NONE           |                          | *NONE   |
| AVG               | *SECOFR    | *ENABLED | *NO                | 160712                         | 220826                          | 0                       | *USRPRF | *NONE         | *NONE           | Arturo Villarroel        | *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL |
| DUTCH             | *SECOFR    | *ENABLED | *NO                | 200601                         | 201122                          | 0                       | *USRPRF | *NONE         | *NONE           | Dutch SP                 | *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL |
| DUTCH1            | *USER      | *ENABLED | *NO                | 200706                         | 200706                          | 0                       | *USRPRF | *NONE         | *NONE           | Dutch SP                 | *NONE   |
| GRACE             | *SECOFR    | *ENABLED | *NO                | 200601                         | 220325                          | 0                       | *USRPRF | *NONE         | *NONE           | Grace                    | *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL |
| KAPILA            | *SECOFR    | *ENABLED | *NO                | 180926                         | 221014                          | 0                       | *USRPRF | *NONE         | *NONE           | Kapila                   | *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL |
| PMBBASIC          | *USER      | *ENABLED | *NO                | 220705                         | 221018                          | 0                       | *USRPRF | *NONE         | *NONE           | Test profile - no spcaut | *NONE   |
| PMBGRP            | *USER      | *ENABLED | *NO                | 220408                         |                                 | 0                       | *USRPRF | *NONE         | *NONE           |                          | *NONE   |
| PMBMYUSR          | *SECOFR    | *ENABLED | *NO                | 220913                         | 220913                          | 0                       | *USRPRF | *NONE         | *NONE           |                          | *ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS                          |

Previous 1 Next

50 entries 1 to 50 / 18

|               |   |   |      |           |
|---------------|---|---|------|-----------|
| Configuration | All Deletions of External Objects on the System are Audited | 1 | Pass | Completed |
| Configuration | Actions that Affect a Job are Audited                       | 0 | Fail | Completed |
| Configuration | Networking and Communications Functions are Audited         | 0 | Fail | Completed |

Search...

Previous 1 Next

50 entries 1 to 50 / 12

ACCESS TO DATA

=> IFS / Object-level Schemas

TGSE1  
PMB

# Work with Authority Schema Detail

4/17/2023  
2:54:47

Schema ID. . : PMBIFS  
Description. : PMB IFS

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

| File<br>Opt | Path or<br>Sys ASP | Library | Object<br>Name | Object<br>Type | Object<br>Owner | Auth<br>List | User<br>Object | Auth     | Exception |
|-------------|--------------------|---------|----------------|----------------|-----------------|--------------|----------------|----------|-----------|
| _           | *IFS /home/pmb     |         |                |                | TGOWNER         | TGAUTL       | *PUBLIC        | *EXCLUDE | *NO       |
| _           | *IFS /home/pmb     |         |                |                | TGOWNER         | TGAUTL       | PMB            | *RWX     | *NO       |
| _           | *IFS /home/pmb     |         |                |                | TGOWNER         | TGAUTL       | TGOWNER        | *RWX     | *NO       |

Bottom

F1=Help F3=Exit F6=Create F7=Report F8=Subset F10=Sort F12=Cancel

MA A

13/004

# Authority Compliance Report(Enforcement=\*NO)



|       |       |            |          |
|-------|-------|------------|----------|
| TGSE1 | ADMIN | 2023-04-18 | 02:34:10 |
|-------|-------|------------|----------|

Search...

Q

Color references: Object current value Schema expected value

| Schema ID | Out of Compliance Reason   | File System | IFS Path    | Auxiliary Storage Pool | Library Name | Object Name | Object Type | Authority List | Schema Authority List | Program Adopt | Schema Program Adopt | Program Adopt Users | Schema Program Adopt Users | Object Owner | Schema Object Owner | Object Primary Group | Schema Object Primary Group | User Inheritance Group | User Name | Schema User Name | Object Authority | Sche Obje |
|-----------|--|-------------|-------------|------------------------|--------------|-------------|-------------|----------------|-----------------------|---------------|----------------------|---------------------|----------------------------|--------------|---------------------|----------------------|-----------------------------|------------------------|-----------|------------------|------------------|-----------|
| PMBIFS    | Object owner does not match schema default. It should be TGOWNER             | *IFS        | /home/pmb/. |                        |              |             |             | *NONE          | TGAUTL                |               |                      |                     |                            | PMB          | TGOWNER             | *NONE                | *SAME                       |                        |           |                  |                  |           |
| PMBIFS    | Object authorization list does not match schema default. It should be TGAUTL | *IFS        | /home/pmb/. |                        |              |             |             | *NONE          | TGAUTL                |               |                      |                     |                            | PMB          | TGOWNER             | *NONE                | *SAME                       |                        |           |                  |                  |           |

02:34:10

C

Color references: Object current value Schema expected value

|        |  |      |             |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--------|--|------|-------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|        | should be TGAUTL   |      |             |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| PMBIFS | Object data authority for user does not match schema default. It should be *EXCLUDE      | *IFS | /home/pmb/. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| PMBIFS | Object management authority for user does not match schema default. It should be removed | *IFS | /home/pmb/. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| PMBIFS | Object manag   | *IFS | /home/pmb/. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

50 entries 1 to 50 / 42

ACCESS TO DATA

=> Network Security

[Dashboard](#)
[Server Management](#)
[Servers](#)
[Server Groups](#)
[Rules](#)
[Job Activity Monitor](#)
[Network Security](#)
[Socket Rules](#)
[Remote Exit Rules](#)
[Exit Point Config](#)
[Defaults](#)
[Access Escalation Mgmt.](#)
[Inactive Sess. Lockdown](#)
[Resource Manager](#)
[User Profile Manager](#)
[Detect Monitors](#)
[Database Encryption](#)

### Network Activity

✕ Reset Filter

▼ Filter

🔄 Refresh(53)

Show 50 entries

Search



| Server | Type | User      | OP Server | Function | SSL | Client IP   | Count | Action   | Object Details       | Timestamp           | Show   |
|--------|------|-----------|-----------|----------|-----|-------------|-------|----------|----------------------|---------------------|--------|
| TGSE1  | *TRN | PMB       | FTPSRV    | SEND     | N/A | 10.11.12.33 | 4     | *PASS    | /finance/Payroll.txt | 2023-04-18-03.12.36 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LIST     | N/A | 10.11.12.33 | 1     | *PASS    | /finance             | 2023-04-18-03.06.13 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | CD       | N/A | 10.11.12.33 | 1     | *PASS    | /finance             | 2023-04-18-03.05.57 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | CD       | N/A | 10.11.12.33 | 1     | *PASS    | /financ              | 2023-04-18-03.05.52 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LIST     | N/A | 10.11.12.33 | 1     | *PASS    | QSYS/QGPL.LIB        | 2023-04-18-03.05.31 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LOGON    | N/A | 10.11.12.33 | 2     | *PASS    |                      | 2023-04-18-03.02.17 | Action |
| TGSE1  | *TRN | QTCP      | FTPSRV    | INIT     | N/A | 10.11.12.33 | 7     | *PASS    |                      | 2023-04-18-03.02.12 | Action |
| TGSE1  | *SOC | QTCP      | ftp       |          | NO  | 10.11.12.33 | 7     | *EXITLVL |                      | 2023-04-18-03.02.11 | Action |
| TGSE1  | *TRN | PMB       | FILE      | ALLOCON  | N/A | 10.11.12.33 | 15    | *PASS    |                      | 2023-04-18-02.32.59 | Action |
| TGSE1  | *TRN | ANONYMOUS | TELNET    | INIT     | N/A | 10.11.12.33 | 54    | *PASS    |                      | 2023-04-18-02.07.13 | Action |
| TGSE1  | *TRN | PMB       | RMTCMD    | PROGRAM  | N/A | 10.11.12.33 | 23    | *PASS    | QSYS/QSYCKUFU.PGM    | 2023-04-18-02.07.12 | Action |
| TGSE1  | *SOC | QUSER     | as-rmtcmd |          | NO  | 10.11.12.33 | 41    | *EXITLVL |                      | 2023-04-18-         | Action |



Dashboard

Server Management

Rules

- Job Activity Monitor
- Network Security
  - Socket Rules
  - Remote Exit Rules
  - Exit Point Config
  - Defaults
- Access Escalation Mgmt.
- Inactive Sess. Lockdown
- Resource Manager
- User Profile Manager
- Detect Monitors
- Database Encryption

Groups

Calendar

Reporting

Activity

Real-time Events

- Network Activity
- Detect Activity
- Alert

Admin

Network Activity

Reset Filter

Filter

Refresh(45)

Show 50 entries

Search

| Server | Type | User      | OP Server | Function | SSL | Client IP   | Count | Action   | Object Details  | Timestamp           | Show   |
|--------|------|-----------|-----------|----------|-----|-------------|-------|----------|---|---------------------|--------|
| TGSE1  | *TRN | PMB       | FILE      | LISTATT  | N/A | 10.27.81.23 | 652   | *PASS    | /TrinityGuard/Reports   | 2023-04-18-13.07.03 | Action |
| TGSE1  | *TRN | PMB       | FILE      | LISTATT  | N/A | 10.27.81.23 | 7     | *PASS    | /TrinityGuard   | 2023-04-18-13.07.02 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LOGON    | N/A | 10.27.81.23 | 3     | *FAIL    |   | 2023-04-18-12.49.20 | Action |
| TGSE1  | *TRN | QTCP      | FTPSRV    | INIT     | N/A | 10.27.81.23 | 3     | *PASS    |   | 2023-04-18-12.49.14 | Action |
| TGSE1  | *SOC | QTCP      | ftp       |          | NO  | 10.27.81.23 | 3     | *EXITLVL |   | 2023-04-18-12.49.14 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | SEND     | N/A | 10.27.81.23 | 1     | *PASS    | /finance/payroll.txt  | 2023-04-18-12.27.35 | Action |
| TGSE1  | *TRN | PMB       | FILE      | OPEN     | N/A | 10.27.81.23 | 1     | *PASS    | /TrinityGuard/js/sortable.js  | 2023-04-18-12.19.14 | Action |
| TGSE1  | *TRN | PMB       | FILE      | OPEN     | N/A | 10.27.81.23 | 1     | *PASS    | /TrinityGuard/Images/help.jpg                                       | 2023-04-18-12.19.13 | Action |
| TGSE1  | *TRN | PMB       | FILE      | OPEN     | N/A | 10.27.81.23 | 1     | *PASS    | /TrinityGuard/Images/TG.jpg   | 2023-04-18-12.19.13 | Action |
| TGSE1  | *TRN | PMB       | FILE      | OPEN     | N/A | 10.27.81.23 | 3     | *PASS    | /TrinityGuard/Reports/Sys_Val_Config_Sys_Val_Compliance_438937.html | 2023-04-18-12.19.13 | Action |
| TGSE1  | *TRN | PMB       | FILE      | ALLOCON  | N/A | 10.27.81.23 | 2     | *PASS    |   | 2023-04-18-11.18.35 | Action |
| TGSE1  | *SOC | QSECOFR   | sftp      |          | YES | 10.27.81.23 | 1     | *EXITLVL |   | 2023-04-18-10.38.34 | Action |
| TGSE1  | *TRN | ANONYMOUS | TELNET    | INIT     | N/A | 10.27.81.23 | 7     | *PASS    |   | 2023-04-18-09.32.10 | Action |
| TGSE1  | *TRN | ANONYMOUS | TELNET    | INIT     | N/A | 10.11.12.33 | 56    | *PASS    |   | 2023-04-18-05.46.00 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | SEND     | N/A | 10.11.12.33 | 4     | *PASS    | /finance/Payroll.txt  | 2023-04-18-03.12.36 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LIST     | N/A | 10.11.12.33 | 1     | *PASS    | /finance  | 2023-04-18-03.06.13 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | CD       | N/A | 10.11.12.33 | 1     | *PASS    | /finance  | 2023-04-18-03.05.57 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | CD       | N/A | 10.11.12.33 | 1     | *PASS    | /financ   | 2023-04-18-03.05.52 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LIST     | N/A | 10.11.12.33 | 1     | *PASS    | QSYS/QGPLLIB  | 2023-04-18-03.05.31 | Action |
| TGSE1  | *TRN | PMB       | FTPSRV    | LOGON    | N/A | 10.11.12.33 | 2     | *PASS    |   | 2023-04-18-03.02.17 | Action |
| TGSE1  | *TRN | QTCP      | FTPSRV    | INIT     | N/A | 10.11.12.33 | 7     | *PASS    |   | 2023-04-18-03.02.12 | Action |
| TGSE1  | *SOC | QTCP      | ftp       |          | NO  | 10.11.12.33 | 7     | *EXITLVL |   | 2023-04-18-03.02.11 | Action |
| TGSE1  | *TRN | PMB       | FILE      | ALLOCON  | N/A | 10.11.12.33 | 15    | *PASS    |   | 2023-04-18-02.32.59 | Action |
| TGSE1  | *TRN | PMB       | RMTCMD    | PROGRAM  | N/A | 10.11.12.33 | 23    | *PASS    | QSYS/QSYCKUFU.PGM   | 2023-04-18-02.07.12 | Action |
| TGSE1  | *SOC | QUSER     | as-rmtcmd |          | NO  | 10.11.12.33 | 41    | *EXITLVL |   | 2023-04-18-02.07.11 | Action |
| TGSE1  | *SOC | QUSER     | as-signon |          | NO  | 10.11.12.33 | 73    | *EXITLVL |   | 2023-04-18-02.07.11 | Action |
| TGSE1  | *TRN | PMB       | FILE      | OPEN     | N/A | 10.11.12.33 | 1     | *PASS    | /TrinityGuard/Reports/Journal_DS_BASE_431269.json                   | 2023-04-17-23.47.35 | Action |
| TGSE1  | *TRN | PMB       | FILE      | LISTATT  | N/A | 10.11.12.33 | 26    | *PASS    | /TrinityGuard   | 2023-04-17-23.47.34 | Action |
| TGSE1  | *TRN | PMB       | FILE      | LISTATT  | N/A | 10.11.12.33 | 1664  | *PASS    | /TrinityGuard/Reports   | 2023-04-17-23.47.28 | Action |
| TGSE1  | *SOC | QUSER     | as-srvmap |          | NO  | 10.11.12.33 | 112   | *EXITLVL |   | 2023-04-17-23.36.09 | Action |

# Privileged Access Management

- Blueprints
- Inactive Profiles
- Access Escalation Management
- Command Security

Dashboard

Server Management

Rules

Job Activity Monitor

Network Security

Access Escalation Mgmt.

Inactive Sess. Lockdown

Resource Manager

User Profile Manager

Blueprints

User Exclusions

Archived Profiles

Create/Change User Profile  
(TGPRFMGR)

Profile Inactivity Settings

Password Rule Settings

Defaults

## Work with Blueprints

+Add ✕ Reset Filter ▼ Filter ↻ Refresh

Show 5 entries

Search 

| Server                 | Blueprint Id | User Group | Prf Parm | Prf Auth | Auth List | 3rd Party | Alt Sts | Compliance Date   | Inact Ovr | Comp Status | Blueprint Description          | Action   |
|------------------------|--------------|------------|----------|----------|-----------|-----------|---------|-------------------|-----------|-------------|--------------------------------|----------|
| TGSE1.TRINITYGUARD.COM | DEVELOPERS   | :DEVELOPER | *YES     | *NO      | *YES      | *NO       | *YES    | 2023-04-18 1:59:5 | *NO       | *FAIL       | Developer User Profile Details | Action ▼ |
| TGSE1.TRINITYGUARD.COM | DUST         | :CASTLE    | *YES     | *NO      | *YES      | *YES      | *NO     | 2023-04-18 1:59:5 | *NO       |             | in the wind                    | Action ▼ |
| TGSE1.TRINITYGUARD.COM | TELLERS      | :TELLERS   | *YES     | *NO      | *YES      | *NO       | *YES    | 2023-04-18 1:59:5 | *NO       | *FAIL       | Teller user                    | Action ▼ |
| TGSE1.TRINITYGUARD.COM | TEST         | :HELPDESK  | *YES     | *NO      | *NO       | *NO       | *YES    | 2023-04-18 1:59:5 | *NO       | *FAIL       | Test                           | Action ▼ |

First 1 Last

Profile Parameters

Profile Authority

Auth Lists

3rd Party

Inact Overrides

Users

Non-comp Profiles

Blueprint permissions


TGCentral perm

Activity

## Parameter settings of TGSE1.TRINITYGUARD.COM TELLERS

+Add Parameter +Add Suggested +Add all defaults ↻ Refresh

Show 20 entries

Search 

| Parameter Description | Parameter Keyword | Parameter Value | Single (Y) | Action   |
|-----------------------|-------------------|-----------------|------------|----------|
| Assistance level      | ASTLVL            | *SYSVAL         | Y          | Action ▼ |
| Limit capabilities    | LMTCPB            | *YES            | Y          | Action ▼ |
| User Class            | USRCLS            | *USER           | Y          | Action ▼ |

First 1 Last



## Blueprint Compliance Report



TGSE1

ADMIN

2023-04-18

02:16:33

Search...



| Blueprint Id | User Name | Violation Category *PARM,*AUT,*AUTL | Violation Keyword | Violation Description | Current Value | Blueprint Value | Non-Compliance Reason  | Action Status | Action Error Details |
|--------------|-----------|-------------------------------------|-------------------|-----------------------|---------------|-----------------|--|---------------|----------------------|
| TELLERS      | PMBBASIC  | *PARM                               | LMTCPB            | Limit capabilities    | *NO           | *YES            | Limit capabilities should be *YES                            |               |                      |
| TELLERS      | PMBBASIC  | *AUTL                               | TGAUTL            | Authority List        |               | *USE            | *USE authoriy should be granted to authorization list TGAUTL |               |                      |
| TELLERS      | PMB1      | *PARM                               | LMTCPB            | Limit capabilities    | *NO           | *YES            | Limit capabilities should be *YES                            |               |                      |
| TELLERS      | PMB1      | *AUTL                               | TGAUTL            | Authority List        |               | *USE            | *USE authoriy should be granted to authorization list TGAUTL |               |                      |
| TELLERS      | PMB2      | *PARM                               | LMTCPB            | Limit capabilities    | *NO           | *YES            | Limit capabilities should be *YES                            |               |                      |
| TELLERS      | PMB2      | *PARM                               | USRCLS            | User Class            | *SYSOPR       | *USER           | User Class should be *USER                                   |               |                      |
| TELLERS      | PMB2      | *AUTL                               | TGAUTL            | Authority List        |               | *USE            | *USE authoriy should be granted to authorization list TGAUTL |               |                      |

Previous

1

Next

50



entries 1 to 50 / 7

[Dashboard](#)
[Server Management](#)
[Rules](#)

▶ Job Activity Monitor

▶ Network Security

▶ Access Escalation Mgmt.

▶ Inactive Sess. Lockdown

▶ Resource Manager

▶ User Profile Manager

[Blueprints](#)
[User Exclusions](#)
[Archived Profiles](#)
[Create/Change User Profile  
\(TGPRFMGR\)](#)
[Profile Inactivity Settings](#)
[Password Rule Settings](#)
[Defaults](#)

### Work with Blueprints

Show 5 entries

#### Server

TGSE1.TRINITYGUARD.COM

TGSE1.TRINITYGUARD.COM

TGSE1.TRINITYGUARD.COM

TGSE1.TRINITYGUARD.COM

First 1 Last

Profile Parameters Profile Au


Parameter settings of TGSE1.T


Show 20 entries


| Parameter Description | Parameter Keyword | Parameter Value | Single (Y) | Action |
|-----------------------|-------------------|-----------------|------------|--------|
| Assistance level      | ASTLVL            | *SYSVAL         | Y          | Action |
| Limit capabilities    | LMTCPB            | *YES            | Y          | Action |
| User Class            | USRCLS            | *USER           | Y          | Action |


First 1 Last


Blueprint/Inactivity Compliance (TGPRFCMP)

**Server**  
 TGSE1.TRINITYGUARD.COM

**Component**  
 TELLERS

**Audit Report**  
 \*YES

**Enforcement**  
 \*NO

**Run interactively**  
 \*YES

Cancel Run

+Add ✕ Reset Filter Filter Refresh

Search

| pliance     | Inact<br>Ovr | Comp<br>Status | Blueprint<br>Description          | Action |
|-------------|--------------|----------------|-----------------------------------|--------|
| 4-18 1:59:5 | *NO          | *FAIL          | Developer User<br>Profile Details | Action |
| 4-18 1:59:5 | *NO          |                | in the wind                       | Action |
| 4-18 1:59:5 | *NO          | *PASS          | Teller user                       | Action |
| 4-18 1:59:5 | *NO          | *FAIL          | Test                              | Action |

ent permissions TGCentral perm Activity

+Add Parameter +Add Suggested +Add all defaults Refresh

Search

[Dashboard](#)
[Server Management](#)
[Rules](#)
[Job Activity Monitor](#)
[Network Security](#)
[Access Escalation Mgmt.](#)
[Inactive Sess. Lockdown](#)
[Resource Manager](#)
[User Profile Manager](#)
[Blueprints](#)
[User Exclusions](#)
[Archived Profiles](#)
[Create/Change User Profile  
\(TGPRFMGR\)](#)
[Profile Inactivity Settings](#)
[Password Rule Settings](#)
[Defaults](#)

### Profile Inactivity Settings

Show 5 entries

#### Server

TGQE5.TRINITYGUARD.COM

TGSE1.TRINITYGUARD.COM

First 1 Last

### Activity History TGSE1.TRINITYGUARD.COM


Show 20 entries

#### Server

First Last

### Edit Profile Inactivity Settings

#### Server

 TGSE1.TRINITYGUARD.COM

#### Inactivity until User Profile is disabled

 30

#### Inactivity until User Profile is deleted

 90


#### Delete profiles with password of \*NONE

 \*NO


#### Object owner for objects owned by deleted profiles

 QDFTOWN

#### Remove deleted Profiles from TG User Group

 \*NO

#### Remove deleted Profiles from TG Rules

 \*NO

#### Alert when Inactivity is found

 \*YES

Cancel

Save

Refresh

Search


Remove deleted  
Profiles from TG  
User Group

Remove deleted  
Profiles from  
TG Rules

Alert when  
Inactivity is  
found

Action

\*NO

\*NO

Action

\*NO

\*YES

Action

Refresh

Search



Status

Dashboard

Server Management

Rules

Job Activity Monitor

Network Security

Access Escalation Mgmt.

Entitlements

Access Control

File Editors

Defaults

Inactive Sess. Lockdown

Resource Manager

User Profile Manager

Detect Monitors

Database Encryption

## Entitlements

+ Add

Refresh

Show 5 entries

Search

Q

| Server                 | Enabled Status | User     | Object    | Library | Type | Swap User | Calendar | Aut Req | Alr Req | Description   | Action |
|------------------------|----------------|----------|-----------|---------|------|-----------|----------|---------|---------|---|--------|
| TGSE1.TRINITYGUARD.COM | Y              | ARP1     | DSPUSRPRF | QSYS    | *CMD | QSECOFR   | *NONE    | Y       | Y       | test  | Action |
| TGSE1.TRINITYGUARD.COM | Y              | PMBBASIC | DSPUSRPRF | QSYS    | *CMD | QSECOFR   | *NONE    | Y       | Y       | Programmer needs ability to view user profile details | Action |

First 1 Last

## Activity History TGSE1.TRINITYGUARD.COM PMBBASIC

Refresh

Show 20 entries

Search

Q

| Server                 | Description                            | Date                | Status     |
|------------------------|--|---------------------|------------|
| TGSE1.TRINITYGUARD.COM | Entitlement for user PMBBASIC imported | 2023-04-18 02:35:38 | *COMPLETED |

First 1 Last

TGSE1  
PMB

# Work with Command Security

4/18/2023  
12:15:13

Subset Criteria - CMD: \*ALL      User : \*ALL      CL.IP: \*ALL      Calendar: \*ALL      ParmRest.: \*ALL      Audit: \*ALL  
                                 Lib: \*ALL      Action: \*ALL      Desc.: \*ALL      Enb.Stat: \*ALL      ExitInst.: \*ALL      Alert: \*ALL

2=Edit 4=Delete 10=Work with Parameters

Position to: \_\_\_\_\_

| Opt | Enable<br>Sts | Command | Library | User    | Client IP | Calendar | Parm<br>Rest | Audit<br>Sts | Alert<br>Sts | Exit<br>Inst | Action | Command Description        |
|-----|---------------|---------|---------|---------|-----------|----------|--------------|--------------|--------------|--------------|--------|----------------------------|
| —   | Y             | STRSQL  | QSQL    | *PUBLIC | *ALL      | *NONE    | *NO          | *YES         | *YES         | *YES         | *FAIL  | Start SQL Interactive Sess |
| —   | Y             | STRSQL  | QSQL    | :ADMINS | *ALL      | *NONE    | *NO          | *YES         | *NO          | *YES         | *PASS  | Start SQL Interactive Sess |

Bottom

F1=Help F2=Add Exit F3=Exit F6=Add F8=Subset F10=Sort F12=Cancel

MA A

12/003



TGSE1  
PMB

Work with Command Security - Edit Record

4/18/2023  
12:15:13

|                        |                  |   |  |
|------------------------|------------------|---|--|
| Command Name . . . . . | : <u>STRSQL</u>  | + | Description: Start SQL Interactive Session |
| Command Library . . .  | : <u>QSQL</u>    |   |  |
| User Name . . . . .    | : <u>:ADMINS</u> | + |  |
| Client IP . . . . .    | : <u>*ALL</u>    |   |  |
| Enable Status . . . .  | : <u>Y</u>       |   | (Y, N)                                     |
| Audit Status . . . .   | : <u>*YES</u>    |   | (*YES, *NO)                                |
| Alert Status . . . .   | : <u>*NO</u>     |   | (*YES, *NO)                                |
| Calendar . . . . .     | : <u>*NONE</u>   | + |  |
| Action . . . . .       | : <u>*PASS</u>   |   | (*FAIL,*PASS)                              |
| Parameter Restriction: | : <u>*NO</u>     |   | (*YES, *NO)                                |
| Exit Installed . . . . | : <u>*YES</u>    |   | (*YES, *NO)                                |

F1=Help F3=Exit F4=Prompt F12=Cancel

# System Value Management

TGSE1

PMB

Work with System Values

4/18/2023

12:18:11

Subset Criteria   Sys.Value: \*ALL   Description: \*ALL   Cur.Value: \*ALL  
Category : \*ALL   Compl.Sts. : \*ALL   Alert: \*ALL   Exp.Value:

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 |
|-----|--------------|----------|---------------------------|----------|----------------|---------------|-----------|
| —   | QPWDCHGBLK   | *SEC     | Block password change     | *NO      | *NONE          | *NONE         | *PASS     |
| —   | QPWDEXPTY    | *SEC     | Password expiration inter | *NO      | 30             | *NOMAX        | *FAIL     |
| —   | QPWDEXPMRN   | *SEC     | Password expiration warni | *NO      | 7              | 7             | *PASS     |
| —   | QPWDLMTAJC   | *SEC     | Limit adjacent digits in  | *NO      | 1              | 0             | *FAIL     |
| —   | QPWDLMTCHR   | *SEC     | Limit characters in passw | *NO      | *NONE          | *NONE         | *PASS     |
| —   | QPWDLMTREP   | *SEC     | Limit repeating character | *NO      | 0              | 0             | *PASS     |
| —   | QPWDLVL      | *SEC     | Password level            | *NO      | 0              | 0             | *PASS     |
| —   | QPWDMAXLEN   | *SEC     | Maximum password length   | *NO      | 8              | 10            | *FAIL     |
| —   | QPWDMINLEN   | *SEC     | Minimum password length   | *NO      | 7              | 6             | *FAIL     |
| —   | QPWDPOSDIF   | *SEC     | Limit password character  | *NO      | 0              | 0             | *PASS     |
| —   | QPWDRQDDGT   | *SEC     | Require digit in password | *NO      | 0              | 0             | *PASS     |
| —   | QPWDRQDDIF   | *SEC     | Duplicate password contro | *NO      | 0              | 0             | *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

MA A

12/003



# Next Steps

- ✓ Free Security Assessment
- ✓ Penetration Test

**Have a project in mind? Questions?**

Let us know in the exit survey, or get in touch:

**[pauline.ayala@freschesolutions.com](mailto:pauline.ayala@freschesolutions.com)**

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