

# CIS IBM i V7R2M0 Benchmark

v1.0.1 - 03-30-2020

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

## Table of Contents

|                                 |     |
|---------------------------------|-----|
| Terms of Use .....              | 1   |
| Overview .....                  | 3   |
| Intended Audience .....         | 3   |
| Consensus Guidance.....         | 4   |
| Typographical Conventions ..... | 5   |
| Scoring Information .....       | 5   |
| Profile Definitions .....       | 6   |
| Acknowledgements .....          | 7   |
| Recommendations .....           | 8   |
| Appendix: Summary Table .....   | 146 |
| Appendix: Change History .....  | 150 |

# Overview

This standard provides the baseline security requirements for IBM i systems.

An owner must be designated for IBM i electronic information assets including the programs and the data labeled as Confidential or Highly Restricted as defined by the company's data classification. The owner must designate an administrator who is responsible for the secure configuration and maintenance. Privileges to modify the functionality and services supported by the IBM i must be restricted to the administrator and approved by the IBM i owner.

Roles and responsibilities on the IBM i must be clearly defined and documented, and address system, application and data security and operational responsibilities. Roles must include resource owners who are responsible for ensuring that appropriate security controls are defined, implemented and maintained and are ultimately accountable for security, access and performance on their designated resource. Development and production roles and responsibilities must be kept separate to ensure an appropriate segregation of duties. Security administration and/or audit roles and responsibilities should be defined to provide validation of activities performed by the administrators and other privileged users.

## Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Intended Audience

These standards apply to all applications, databases and connections to the IBM i.

## Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention                           | Meaning   |
|--------------------------------------|---|
| <code>Stylized Monospace font</code> | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| Monospace font                       | Used for inline code, commands, or examples. Text should be interpreted exactly as presented.           |
| < <i>italic font in brackets</i> >   | Italic texts set in angle brackets denote a variable requiring substitution for a real value.           |
| <i>Italic font</i>                   | Used to denote the title of a book, article, or other publication.                                      |
| <b>Note</b>                          | Additional information or caveats   |

## Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

### Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

### Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

**Corporate/Enterprise Environment (general use)**

Items in this profile intend to:

```
-be practical and prudent;  
  
-provide a clear security benefit; and  
  
-not negatively inhibit the utility of the technology beyond acceptable means.
```

- **Level 2**

**High Security/Sensitive Data Environment (limited functionality)**

Items in this profile may have the following characteristic(s):

```
-are intended for environments or use cases where security is paramount  
  
-acts as defense in depth measure  
  
-may negatively inhibit the utility or performance of the technology.
```

## Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

### **Author**

Bruce Bading

### **Contributor**

Terry Ford

Thomas Barlen

Robert Andrews

Dan Riehl

Eric Pinnell

Bruce Bading

### **Editor**

Matthew Woods



# Recommendations

## ***1 Access Control***

The following paragraphs define the controls and parameters for access control to the IBM i and its resources.

Critical, sensitive, confidential and/or highly restricted objects must be \*EXCLUDEd from the \*PUBLIC and private authorities, group authorities and/or authorization lists must be used to secure these objects. The minimum authority required to perform specific functions must be granted and excessive authorities must be removed.

Periodic reviews of critical, sensitive, confidential and/or highly restricted objects must be performed to ensure that proper access control is maintained.

## ***2 Adopted Authority***

You should use adopted authorities with care to prevent possible security risks. Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user will not normally have. Adopted authority provides an important tool for meeting diverse authority requirements, but it should be used with care:

[https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarladprskrcm dt.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarladprskrcm dt.htm)

- Adopt the minimum authority required to meet the application requirements using the Principle of Least Privilege (PoLP). Adopting the authority of an application owner is preferable to adopting the authority of QSECOFR or a user with any special authorities, especially \*ALLOBJ.
- Carefully monitor the function provided by programs that adopt authority. Make sure that the programs do not provide a means for the user to access objects outside the control of the program, such as command line entry capability.
- Make sure that programs that adopt authority and call other programs perform library qualified calls. Do not use the library list (\*LIBL) on the call.
- Control which users are permitted to call programs that adopt authority. Use menu interfaces and library security to prevent these programs from being called without sufficient control.
- Administrative and third-party libraries such as Profile and System Administration, High Availability and Change Management libraries that contain programs that adopt powerful special authorities shall be controlled with \*PUBLIC \*EXCLUDE

access and grant only authorized user/groups access whose job roles require such access.

### 3 User Profiles

User Profiles provide identity authentication into your system. Designing them well can help you protect your system and customize it for your users. Each user profile is a \*USRPRF object in system library QSYS, that contains a password, several security related parameters and a list of the objects the user owns.

Following are important aspects of IBM i user profiles that you should consider to properly secure your systems.

- Every user profile should be unique (no shared accounts).
- Every user should have a unique and non-trivial password of sufficient strength and complexity.
- Each individual user profile should have authorities and privileges commensurate with their specific job role.
  - o There are a total of eight administrative special authorities and each administrator should have the minimum special authority commensurate with their job role.
  - o Application users and groups should have no Special Authorities (\*NONE) and be granted proper authority to resources (objects and file) commensurate with their job role.
- All \*USRPRF objects should be authorized only to the \*USRPRF owner and the user profile itself and the \*PUBLIC authority should be \*EXCLUDE and no private authorities should be granted to any \*USRPRF objects.

[https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlusrprf.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlusrprf.htm)  
[https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlspcaut.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlspcaut.htm)

#### 3.1 (L1) User Profile (\*USRPRF) Access Controls (\*PUBLIC authority) (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Your most important protection is resource security on your server. Resource security on the system allows you to define who can use objects and how those objects can be used.

Every user profile exists as a \*USRPRF object in library QSYS. Granting authorities to \*USRPRF objects allows those who have been granted authority to hijack those users without proper authentication (no password). Jobs submitted or swapped as other \*USRPRF objects will inherit their privileges and authorities. The default \*PUBLIC authority (AUT) to all user profile objects (\*USRPRF) is \*EXCLUDE and should never be changed to prevent anyone other than the owner and the user profile itself from using it to gain unauthorized access to \*USRPRF objects including all authorizations and privileges without knowing the password.

\*PUBLIC authority to all user profiles should be \*EXCLUDE with the following exceptions:

QDBSHR QDBSHRDO QTMPLPD

### **Rationale:**

Granting the \*PUBLIC an authority greater than \*EXCLUDE to any \*USRPRF object allows an attacker to swap with or submit jobs as these profiles and use their privileges and authorizations without knowing their passwords or credentials. \*PUBLIC refers to all authenticated users. Granting the \*PUBLIC authority to any profile other than QDBSHR, QDBSHRDO and QTMPLPD is a security risk.

### **Audit:**

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT ALL  
SYS_ONAME, OBJTYPE, USER_NAME, OBJ_AUTH  
FROM QSYS2/OBJ_PRIV T01  
WHERE OBJTYPE = '*USRPRF'  
AND SYS_ONAME NOT IN ('QDBSHR', 'QDBSHRDO', 'QTMPLPD')  
AND USER_NAME = '*PUBLIC'  
AND OBJ_AUTH <> '*EXCLUDE'
```

- Verify that the display returns no \*PUBLIC authorized objects.

### **Remediation:**

To establish the recommended configuration, change any \*USRPRF objects identified in the audit to the default shipped and creation value \*EXCLUDE to secure all user profiles from malicious use.

```
GRTOBJAUT OBJ(<xxxxxx>) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE)  
REPLACE(*YES)
```

### **Impact:**

Functions involving profile swaps and changes may be impacted.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/cl/crtusrprf.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/cl/crtusrprf.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmappl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmappl.htm)

## 3.2 (L1) User Profile (\*USRPRF) Access Controls (Private authority) (Scored)

### Profile Applicability:

- Level 1

### Description:

Your most important protection is resource security on your server. Resource security on the system allows you to define who can use objects and how those objects can be used. Every user profile exists as a \*USRPRF object in library QSYS. Granting authorities to \*USRPRF objects allows those who have been granted authority to hijack those users without proper authentication (no password). Jobs submitted or swapped as other \*USRPRF objects will inherit their privileges and authorities. The default \*PUBLIC authority (AUT) to all user profile objects (\*USRPRF) is \*EXCLUDE and should never be changed to prevent anyone other than the owner and the user profile itself from using it to gain unauthorized access to \*USRPRF objects including all authorizations and privileges without knowing the password.

All Private authorities to all user profiles other than the owner's and the profile itself should be removed:

### Rationale:

Granting a private authority to any \*USRPRF object allows an attacker to swap with or submit jobs as these profiles and use their privileges and authorizations without knowing their passwords or credentials. Granting a private authority to any \*USRPRF object is a security risk.

### Audit:

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT SYS_ONAME, OBJTYPE, USER_NAME, OBJ_AUTH  
FROM QSYS2/OBJ_PRIV LEFT OUTER JOIN QSYS2/GROUPLIST  
ON SYS_ONAME = GROUPNAME  
WHERE OBJTYPE = '*USRPRF'  
AND SYS_ONAME <> USER_NAME  
AND USER_NAME <> OWNER  
AND USER_NAME <> '*PUBLIC'  
AND USERNAME IS NULL
```

AND SYS\_ONAME CONCAT USER\_NAME NOT IN  
( 'QGATEQSNADS', 'QMQMQMQMADM', 'QMSFQTCP',  
'QSPLJOBQSPL', 'QTCPQMSF', 'QTMHHTTPQCLUSTER')

- Verify that the display returns no privately authorized objects.
- o SYSTEM\_OBJECT\_NAME is the \*USRPRF object that is privately authorized to the USER\_NAME profile.

### **Remediation:**

To establish the recommended configuration, change any \*USRPRF (SYSTEM\_OBJECT NAME) objects identified in the audit to the default shipped and creation value \*EXCLUDE to secure all user profiles from malicious use.

RVKOBJAUT OBJ(<xxxxxx>) OBJTYPE(\*USRPRF) USER(<xxxxxx>) AUT(\*ALL)

- Note: Replace xxxxxx for OBJ(<xxxxxx>) with the SYSTEM\_OBJECT\_NAME from the audit
- Replace xxxxxx for USER(<xxxxxx>) with the USER\_NAME from the audit

### **Impact:**

Functions involving profile swaps and changes may be impacted.

### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/cl/crtusrprf.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/cl/crtusrprf.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmस्पpl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmस्पpl.htm)

### 3.3 (L1) User Profile (\*USRPRF) Object Ownership (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

Your most important protection is resource security on your server. Resource security on the system allows you to define who can use objects and how those objects can be used. Every user profile exists as a \*USRPRF object in library QSYS. Granting authorities to \*USRPRF objects allows those who have been granted authority to hijack those users without proper authentication (no password). Jobs submitted or swapped as other \*USRPRF objects will inherit their privileges and authorities. The default \*PUBLIC authority (AUT) to all user profile objects (\*USRPRF) is \*EXCLUDE and should never be changed to prevent anyone other than the owner and the user profile itself from using it to gain unauthorized access to \*USRPRF objects including all authorizations and privileges without knowing the password.

All IBM Supplied Profiles shall be owned by QSYS with the following exceptions:

- QFAXMSF shall be owned by QAUTPROF
- QRDARS400xx shall be owned by QRDARS400
- QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI

Non-IBM (user created) profiles shall be owned by QSECOFR or QSYS.

#### **Rationale:**

Granting ownership authority to any \*USRPRF object allows an attacker to swap with or submit jobs as these profiles and use their privileges and authorizations without knowing their passwords or credentials. Granting ownership authority to any \*USRPRF object is a security risk.

#### **Audit:**

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.  
SELECT ALL SYS\_ONAME, OBJTYPE, OWNER FROM QSYS2/OBJ\_PRIV

WHERE OBJTYPE = '\*USRPRF' AND USER\_NAME = '\*PUBLIC'



AND OWNER NOT IN ('QSECOFR', 'QSYS')

- Verify that the display returns no ownership anomalies with the following valid exceptions.

- QFAXMSF shall be owned by QAUTPROF
- QRDARS400<x> shall be owned by QRDARS400
- QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI

### **Remediation:**

To establish the recommended configuration, change the owner of all non-IBM supplied \*USRPRF objects to QSECOFR:

CHGOBJOWN OBJ() OBJTYPE(\*USRPRF) NEWOWN(QSECOFR) CUROWNAUT(\*REVOKE)

### **Impact:**

Functions involving profile swaps and changes may be impacted.

### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibm\\_sppl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibm_sppl.htm)

### 3.4 (L1) Administrative Special Authorities (Not Scored)

#### Profile Applicability:

- Level 1

#### Description:

Special authority is used to specify the types of actions a user can perform on system resources. A system administrator can be given one or more special authorities directly or through a group. System administrators should be granted administrative special authorities commensurate with their job roles.

#### Rationale:

Special authorities are granted to administrators based on the User class (USRCLS) and Special authority (SPCAUT) fields in the user profile. Based on the Principle of Least Privilege (PoLP), application users (USRCLS = \*USER) should have no administrative special authority (SPCAUT = \*NONE). Granting any of the eight administrative special authorities must be done in consideration with the Principle of Least Privilege (PoLP) as defined by the NIST and regulatory compliance requirements.

#### Audit:

PRTUSRPRF SELECT(\*SPCAUT) SPCAUT(\*ALL)

Type WRKSPLF and locate your spool file with the name QPSECUSR and User Data PRTUSRPRF. View the spool file output to ensure that all administrators listed with Special Authorities have the least privileges commensurate with their administrative job roles. Note that administrative Special Authorities are cumulative from User Profile and Group Profiles.

IBM supplied user profiles will appear in the report and should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

#### Remediation:

To establish the recommended configuration, lower all administrators to the special authorities commensurate with their job roles.

CHGUSRPRF USRPRF(<xxxxxx>) SPCAUT(<xxxxxx>)

Change all non-administrative \*USER class users and groups to SPCAUT = \*NONE:

CHGUSRPRF USRPRF(<xxxxxx>) SPCAUT(\*NONE)

#### Impact:

Administrator functions performed with administrator special authorities may be impacted.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlspc aut.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlspc aut.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibm sppl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibm sppl.htm)
3. <https://csrc.nist.gov/glossary/term/least-privilege>

### *3.5 (L1) User Profile Action Auditing (Scored)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:

- Act as part of the operating system or access system and other sensitive objects
- Back up objects, files and directories
- Restore objects, files and directories
- Take ownership of files or other objects
- Create, change and delete user profiles
- Change priority or end and control system and other user's jobs and spooled files.
- Start System Service Tools, debug programs and perform or alter service functions
- Trace communications and jobs
- Change, view and control system and resource auditing
- Change how the system and communications are configured

Actions of administrative special authorities allow auditors to monitor actions taken by administrators.

#### **Rationale:**

Auditing these events may be useful when investigating a security incident.

The CHGUSRAUD (Change User Audit) command allows a user with audit (\*AUDIT) special authority to set up or change auditing for a user. The system value QAUDCTL controls turning auditing on and off. The auditing attributes of a user profile can be displayed with the Display User Profile (DSPUSRPRF) command.

#### **Audit:**

PRTUSRPRF SELECT(\*SPCAUT) SPCAUT(\*ALL)

Type WRKSPLF to locate your spool file with the name QPSECUSR and User Data PRTUSRPRF. View spool file output and use the DSPUSRPRF command to ensure that all administrators with special authorities have an action auditing value of \*CMD. Note that administrative Special Authorities are cumulative from User Profile and Group Profiles. IBM supplied user profiles with the exception of QSECOFR should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

1. Type DSPUSRPRF For each of the users in the report and examine the action auditing value to ensure that \*CMD action auditing is specified.
2. DSPUSRPRF USRPRF(<xxxxxx>) TYPE(\*BASIC)

### **Remediation:**

To establish the recommended configuration, change the action auditing value of all administrative special authority users to include \*CMD action auditing:

CHGUSRAUD USRPRF(<xxxxxx>) AUDLVL(\*CMD)

### **Impact:**

If no audit settings are configured, or if audit settings are too lax in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlspc aut.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlspc aut.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibm sppl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibm sppl.htm)
3. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/cl/chgusraud. htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/cl/chgusraud. htm)

## 3.6 (L1) Default Passwords (Scored)

### Profile Applicability:

- Level 1

### Description:

When you create a new user profile, the default is to make the password the same as the user profile name. When you create new user profiles, consider assigning a unique, non-trivial password instead of using the default password.

### Rationale:

Default passwords provide an opportunity for someone to enter your system, if someone knows your policy for assigning profile names and knows that a new person is joining your organization. Additionally, accounts with default passwords are often used for shared (non-unique) accounts. Tell the new user the password confidentially, such as in a “Welcome to the System” letter that outlines your security policies. Require the user to change the password the first time that the user signs on by setting the user profile to

**PWDEXP(\*YES).**

### Audit:

- On a command line, type STRSQL and press Enter
- Enter the following SQL statement and press Enter.

```
SELECT ALL  
USER_NAME, STATUS, DFTPWD, PWDEXP  
FROM QSYS2/USER_INFO T01  
WHERE DFTPWD = 'YES'
```

### Remediation:

To establish the recommended configuration, change the password of all user profiles with default passwords to a non-trivial password and set the password to expire.

```
CHGUSRPRF USRPRF(<xxxxxx>) PASSWORD(<xxxxxx>) PWDEXP(*YES)
```

Additionally, the command ANZDFTPWD ACTION (\*DISABLE) should be added to a job schedule entry to periodically scan for and \*DISABLE any profiles with \*DEFAULT passwords, and system value QPWDRULES should contain the parameters \*ALLCRTCHG and \*LMTPRFNAME to prevent the creation of profiles with \*DEFAULT passwords.

### Impact:

Shared passwords may be impacted.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/cl/anzdftpwd.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/cl/anzdftpwd.htm)

### 3.7 (L1) Inactive Profiles (Scored)

#### Profile Applicability:

- Level 1

#### Description:

Remove/disable inactive user profiles within 90 days.

#### Rationale:

Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access sensitive data.

#### Audit:

- On a command line, type STRSQL and press Enter
- Enter the following SQL statement and press Enter.

```
SELECT ALL  
USER_NAME, STATUS, LASTUSED  
FROM QSYS2/USER_INFO T01  
WHERE STATUS = '*ENABLED'  
AND LASTUSED <= "  
OR STATUS = '*ENABLED'  
AND LASTUSED IS NULL
```

Note: In the above SQL, enter the calendar date equal to 90 days prior to the audit or that of your inactive profile policy. The date needs to be entered in 'yyyy-mm-dd' format enclosed in single ' marks as in the following example:

```
LASTUSED <= '2020-01-01'
```

IBM supplied user profiles will appear in the report and should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

#### Remediation:

To establish the recommended configuration, remove/disable all inactive profiles displayed.

```
CHGUSRPRF USRPRF(<xxxxxx>) STATUS(*DISABLED)
```

Optional (recommended) on a regular basis such as 30-90 days after inactive profiles have been \*DISABLED, they should be archived and removed.

```
DLTUSRPRF USRPRF(<xxxxxx>)
```



Note that when removing user profiles, there needs to be consideration of changing ownership of the objects they own.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmस्प्ल.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmस्प्ल.htm)

### 3.8 (L1) User Profile With Non-Expiring Passwords (Not Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

User Profiles with non-expiring passwords are never required to change their password.

#### **Rationale:**

Non-expiring passwords are security risks because if no automated solution is in place, users are never prompted to change their passwords. Non-expiring passwords present a security risk as they may either be shared (non-unique) accounts or their passwords may be easy to obtain through observation of login keystrokes over an indefinite period of time.

#### **Audit:**

- On a command line, type STRSQL and press Enter
- Enter the following SQL statement and press Enter.

```
SELECT ALL  
USER_NAME, STATUS, PWDEXPITV, LASTUSED  
FROM QSYS2/USER_INFO T01  
WHERE PWDEXPITV = -1
```

Service accounts may be excluded from the audit and remediation. A service account is a user account that is created explicitly to provide a security context for automated system and application services running on the system. Service accounts should be configured with a non-trivial, complex password that is used in an automated service process and never used interactively. Service accounts should be documented and their Password expiration interval should be set to \*NOMAX. A process should then be documented and executed to periodically change their passwords manually.

#### **Remediation:**

To establish the recommended configuration, change all interactive user profile password expiration intervals to \*SYSVAL and ensure that your system value for QPWDEXPITV is set to 90 days or less or a value commensurate with your policy:

```
CHGUSRPRF USRPRF(<xxxxxx>) PWDEXPITV(*SYSVAL)
```

#### **Impact:**

Shared accounts may be impacted.

### *3.9 (L1) User Profiles With Command Line Access (Not Scored)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

User Profiles with command line access can run commands they are authorized to from a command line.

#### **Rationale:**

Application user profiles should be limited to menus and restricted from directly running system commands from a command line. Only administrators with Special Authorities limited to the Principle of Least Privilege may be allowed to run commands from a command line.

#### **Audit:**

- On a command line, type STRSQL and press Enter
- Enter the following SQL statement and press Enter.

```
SELECT ALL
```

```
USER_NAME, STATUS, LMTCPB, SPCAUT
```

```
FROM QSYS2/USER_INFO T01
```

```
WHERE LMTCPB <> '*YES'
```

IBM supplied user profiles will appear in the report and should be excluded from the audit.

A list of IBM supplied user profiles can be obtained from the references below.

#### **Remediation:**

To establish the recommended configuration, change all non-administrative application users to command line capability to \*YES:

```
CHGUSRPRF USRPRF(<xxxxxx>) LMTCPB(*YES)
```

#### **Impact:**

Users will be prevented from running command from a command line.

### 3.10 (L1) IBM Supplied User Profiles (Not Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This section contains information about the IBM-Supplied user profiles that are shipped with the system and Licensed Program Products. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

#### **Rationale:**

You must change the password for the QSECOFR profile after you install your system. This password is the same for every IBM i system and poses a security exposure until it is changed. However, Do not change any other values for IBM-supplied user profiles. Changing these profiles can cause system functions to fail. Additionally, IBM Supplied Profiles should not be used as group profiles with few exceptions. It is better to create your own group profiles with the proper authorities and special authorities using the Principle of Least Privilege (PoLP) as defined by the NIST and regulatory compliance requirements.

All IBM-supplied user profiles except for QSECOFR are shipped with a password of \*NONE and are not intended for sign-on. These profiles are used by the IBM i operating system. Therefore, signing on with these profiles or using the profiles to own user (non-IBM supplied ) objects is not recommended.

#### **Audit:**

#### **Changes to IBM Supplied Profiles**

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT AUTHORIZATION_NAME, NO_PASSWORD_INDICATOR, STATUS,  
  
USER_CLASS_NAME, INITIAL_PROGRAM_NAME,  
LIMIT_CAPABILITIES, SPECIAL_AUTHORITIES  
FROM QSYS2/USER_INFO WHERE AUTHORIZATION_NAME LIKE 'Q%' AND  
NO_PASSWORD_INDICATOR = 'NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND STATUS =  
'*DISABLED' OR AUTHORIZATION_NAME LIKE 'Q%' AND USER_CLASS_NAME <> '*USER'  
OR AUTHORIZATION_NAME LIKE 'Q%' AND INITIAL_PROGRAM_NAME <> '*NONE' OR
```

AUTHORIZATION\_NAME LIKE 'Q%' AND LIMIT\_CAPABILITIES <> '\*NO' OR  
AUTHORIZATION\_NAME LIKE 'Q%' AND SPECIAL\_AUTHORITIES <> '\*NONE'

- Review the results of the screen output. This indicates that one or more of the following parameters of the profiles in the list does not match the default values that are used for all IBM-supplied user profiles.
- NO\_PASSWORD\_INDICATOR (PASSWORD) = YES (Default)
- STATUS (STATUS) = \*ENABLED (Default)
- USER\_CLASS\_NAME (USRCLS) = \*USER (Default)
- INITIAL\_PROGRAM\_NAME (INLPGM) = \*NONE (Default)
- LIMIT\_CAPABILITIES (LMTCPB) = \*NO (Default)
- SPECIAL\_AUTHORITIES (SPCAUT) = \*NONE (Default)
- Compare the results of the screen output to information about IBM-supplied profiles, their purpose, and values for any IBM-supplied profiles that are different from the defaults from the shipped defaults from the following link.

[https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmprfa.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmprfa.htm)

### **IBM Supplied Group Profiles**

- To check if IBM Supplied Profiles are being used as Group Profiles
- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT T01.GROUPNAME, T01.USERNAME FROM QSYS2/GROUPLIST T01 INNER JOIN
```

```
QSYS2/USER_INFO T02 ON T01.GROUPNAME = T02.USER_NAME WHERE
```

```
T02.USER_NAME LIKE 'Q%'
```

```
AND T02.USER_NAME NOT IN ('QBRMS', 'QMQMADM', 'QONDADM',  
'QRDARS400', 'QRDARSADM', 'QWQADMIN')
```

- Review the results of the screen output. The following are valid exclusions from the audit.
- QBRMS
- QMQMADM
- QONDADM
- QRDARS400
- QRDARSADM
- QWQADMIN

### **Remediation:**

- Change any IBM-Supplied user profile found in the audit that are different from the defaults or values different from the list in the referenced table  
[https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmsppl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmsppl.htm)

CHGUSRPRF USRPRF(<xxxxxx>) <parameter>(<xxxxxx>)

- Change any User Profile that is a group member of an IBM-Supplied user profile found in the audit to remove the IBM-Supplied user profile from its Group (GRPPRF) and/or Supplemental Group (SUPGRPPRF) parameters.

CHGUSRPRF USRPRF(<xxxxxx>) GRPPRF(<xxxxxx>) SUPGRPPRF(<xxxxxx>)

### Impact:

Functions using the authorities and parameters of any profile you change may fail. You may want to contact IBM or your business partner for guidance prior to making any changes.

### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmprfa.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmprfa.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarldftusrprf.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarldftusrprf.htm)
3. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmsppl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmsppl.htm)

### Notes:

Note: The table includes only some, but not all user profiles for licensed program products; therefore, the list may not be inclusive of all IBM supplied profiles. Contact IBM or an IBM i Business Partner if you have questions or need guidance. Note however that you should also contact an IBM i Security Subject Matter Expert for guidance.

([https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlibmsppl.h](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlibmsppl.htm)  
tm)

### 3.11 (L1) Group Profiles With Passwords (Scored)

#### Profile Applicability:

- Level 1

#### Description:

Group profiles should not have a password as they are usually not associated with a unique account.

#### Rationale:

Unique accounts provide accountability to the actions they perform. Group members should all be unique, but allowing the group profile to which they belong to sign on with a password provides no unique accountability to the actions that shared profiles with a password present.

#### Audit:

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.  
SELECT All

```
T01.GROUPNAME, T02.NOPWD
```

```
FROM QSYS2/GROUPLIST T01 INNER JOIN
```

```
QSYS2/USER_INFO T02
```

```
ON T01.GROUPNAME = T02.USER_NAME
```

```
WHERE T02.NOPWD = 'NO'
```

- Verify that the display returns no group profiles with a password (NOPWD = NO).

#### Remediation:

```
CHGUSRPRF USRPRF(<xxxxxx>) PASSWORD(*NONE)
```

Where USRPRF(<xxxxxx>) in the above example is the group profile/s from the above audit.

## 4 System Configuration

The recommendations that follow detail the IBM i configuration settings.

## ***4.1 Security System Values***

The following recommendations represent the comprehensive standard system settings for the i system.



## **4.1.1 Level 1**

Corporate/Enterprise Environment (general use)

### **4.1.1.1 (L1) Allow Restoration of Security-Sensitive Objects (Scored)**

#### **Profile Applicability:**

- Level 1

#### **Description:**

Determines if the system will allow authorized users to restore system-state objects or programs that adopt authority to the system.

System administrators must use this privileged access to restore objects frequently as a part of their routine IBM-supplied PTF O/S maintenance as well as related to back-up and recover processes for applications. The restore privileges will be limited to System administrator and security personnel based on special authorities.

#### **Rationale:**

Because some programs may cause serious problems, this system value provides a method to protect your system.

#### **Audit:**

DSPSYSVAL SYSVAL(QALWOBJRST)

#### **Remediation:**

To establish the recommended configuration, set the following system value to \*ALWPTF:  
QALWOBJRST

CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('\*ALWPTF')

#### **Impact:**

It is important to set the QALWOBJRST value to \*ALL before performing some system activities, such as:

- Installing a new release of the IBM® i licensed program
- Installing new licensed programs
- Recovering your system

These activities may fail if the QALWOBJRST value is not \*ALL. To ensure system security, return the QALWOBJRST value to your normal setting after completing the system activity.

If you regularly restore programs and applications to your system and accept the risk, you might need to set the QALWOBJRST system value to \*ALWPGMADP. Restoration of programs that adopt authority may pose a security risk to your system and must be evaluated carefully prior to restoring to your system.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqalwrst.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqalwrst.htm)

#### 4.1.1.2 (L1) Set Attention Program (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Determines what program is executed when the user presses the attention-key.  
(Note:\*ASSIST is interpreted by the system to use the QSYS/QEZMAIN program, which is displayed if you view the setting using the PRTSYSSECA command.)

##### **Rationale:**

You can specify the program to call when you press the Attention key.

##### **Audit:**

DSPSYSVAL SYSVAL(QATNPGM)

##### **Remediation:**

To establish the recommended configuration, set the following system value to \*NONE:

QATNPGM

CHGSYSVAL SYSVAL(QATNPGM) VALUE('\*NONE')

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzakz/rzakzqatnpgm.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzakz/rzakzqatnpgm.htm)

### 4.1.1.3 (L1) Set Auditing Control (Scored)

#### Profile Applicability:

- Level 1

#### Description:

Serves as the on/off switch for security auditing. \*AUDLVL activates event auditing at the system or user level. \*OBJAUD activates object auditing. \*NOQTEMP prevents extraneous auditing entries for objects in library QTEMP.

#### Rationale:

Auditing can be defined as an inspection or examination of a process or system to determine the quality of it, and is also used to ensure compliance to requirements.

#### Audit:

DSPSYSVAL SYSVAL(QAUDCTL)

#### Remediation:

To establish the recommended configuration, set the following system value to \*NOQTEMP, \*OBJAUD, \*AUDLVL:

QAUDCTL

CHGSYSVAL SYSVAL(QAUDCTL) VALUE('\*NOQTEMP \*OBJAUD \*AUDLVL')

#### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaudcon.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaudcon.htm)

#### 4.1.1.4 (L1) Set Auditing End Action (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines the action the system should take if it is unable to continue auditing (e.g. the audit record is full).

**Rationale:**

System continues to operate but sends a message to the system operator and to the QSYS/QSYSMSG if the message.

**Audit:**

DSPSYSVAL SYSVAL(QAUDENDACN)

**Remediation:**

To establish the recommended configuration, set the following system value to \*NOTIFY:

QAUDENDACN

CHGSYSVAL SYSVAL(QAUDENDACN) VALUE(\*NOTIFY)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlauditea.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlauditea.htm)

#### 4.1.1.5 (L1) Set Auditing Force Level (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines how many auditing journal entries records are cached in memory before they are physically written to disk from memory.

**Rationale:**

This will provide the best auditing performance and lets the system determine the appropriate setting based on performance history.

**Audit:**

DSPSYSVAL SYSVAL(QAUDFRCLVL)

**Remediation:**

To establish the recommended configuration, set the following system value to \*SYS:

QAUDFRCLVL

CHGSYSVAL SYSVAL(QAUDFRCLVL) VALUE('\*SYS')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlauditfl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlauditfl.htm)

#### 4.1.1.6 (L1) Set Auditing Level (Scored)

##### Profile Applicability:

- Level 1

##### Description:

Determines the level of auditing on the system. At a minimum the following settings must be set;

- \*AUTFAIL – Authority failures.
- \*CREATE – Objects are created
- \*DELETE – Objects are deleted
- \*OBJMGT – Object management tasks.
- \*PGMFAIL - Program failures, i.e. a blocked instruction, validation value failure, domain violation
- \*SAVRST – Save and restore operations,
- \*SECURITY - Security events.
- \*SERVICE – Use of service tools,
- \*SYSMGT – System management tasks

##### Rationale:

This will make it easier to view the security audit journal as it determines which security-related events are logged.

##### Audit:

DSPSYSVAL SYSVAL(QAUDLVL)

##### Remediation:

To establish the recommended configuration, set the following system value to \*AUTFAIL, \*CREATE, \*DELETE, \*OBJMGT, \*PGMFAIL, \*SAVRST, \*SECURITY, \*SERVICE, \*SYSMGT:

QAUDLVL

CHGSYSVAL SYSVAL(QAUDLVL) VALUE(\*AUTFAIL \*CREATE \*DELETE \*OBJMGT \*PGMFAIL \*SAVRST \*SECURITY \*SERVICE \*SYSMGT')

##### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaudlev.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaudlev.htm)

#### 4.1.1.7 (L1) Set Security Auditing Level Extensions (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Allows additional space to specify more than sixteen audit values.

You can specify more than one value for the QAUDLVL2 system value, unless you specify \*NONE. For the QAUDLVL2 system value to take effect, the QAUDCTL system value must include \*AUDLVL and the QAUDLVL system value must include \*AUDLVL2.

**Rationale:**

The Auditing Level Extension (QAUDLVL2) system value is required when more than sixteen auditing values are needed.

**Audit:**

DSPSYSVAL SYSVAL(QAUDLVL2)

**Remediation:**

CHGSYSVAL SYSVAL(QAUDLVL2) VALUE(\*NONE)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaudlev2.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaudlev2.htm)



#### *4.1.1.8 (L1) Set Automatic Device Configuration (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Specifies whether locally attached devices are configured automatically.

**Rationale:**

Automatic configuration changes the device description to match the keyboard attached. You may not want to use automatic configuration if you are using manual configuration to set up a device with a different keyboard type than the hardware reports.

**Audit:**

DSPSYSVAL SYSVAL(QAUTOCFG)

**Remediation:**

To establish the recommended configuration, set the following system value to "0" (OFF):

QAUTOCFG

CHGSYSVAL SYSVAL(QAUTOCFG) VALUE('0')

**Impact:**

Do NOT automatically configure locally attached devices except when configuring new local controllers or devices.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlautocconfig.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlautocconfig.htm)

#### *4.1.1.9 (L1) Set Automatic Remote Controller Configuration (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Determines whether automatic remote workstation controller configuration is enabled.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QAUTORMT)

**Remediation:**

To establish the recommended configuration, set the following system value to "0" (OFF):

QAUTORMT

CHGSYSVAL SYSVAL(QAUTORMT) VALUE('0')

**Impact:**

Do NOT automatically configure remote workstation controllers.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/ssw\\_ibm\\_i\\_72/rzakz/rzakzqauto\\_rmt.htm](https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzakz/rzakzqauto_rmt.htm)

#### *4.1.1.10 (L1) Set Automatic Virtual Device Creation (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Determines whether automatic device creation is allowed and if so, how many devices can be configured automatically. Specify a value 1 through 32500 for this system value and is both sufficient to support the needs of the business and not too large to represent a denial of service exposure since it represents a finite limit. Setting the value to \*NOMAX is a security risk as an infinite number of virtual devices may lead to a denial of service if disk capacity is reached.

**Rationale:**

The value should be sufficient enough that enough devices are allocated to support the business.

**Audit:**

DSPSYSVAL SYSVAL(QAUTOVRT)

**Remediation:**

To establish the recommended configuration, set the following system value to 32500 or less to specify an adequate number of devices to support the business:

QAUTOVRT

CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(<XXXXXX>)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlautovrt.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlautovrt.htm)

#### 4.1.1.11 (L1) Set Create Authority (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Specifies the default public authority.

##### **Rationale:**

This lets the public view newly created objects, but not change them. This will ensure the integrity of the newly created objects. You can override the QCRTAUT system value at a library level to specify data classifications within specific application libraries.

##### **Audit:**

DSPSYSVAL SYSVAL(QCRTAUT)

##### **Remediation:**

To establish the recommended configuration, set the following system value to \*USE:

QCRTAUT

CHGSYSVAL SYSVAL(QCRTAUT) VALUE('\*USE')

##### **Impact:**

Several IBM-supplied libraries, including QSYS, have a CRTAUT value of \*SYSVAL. If you change the QCRTAUT system value to something other than \*CHANGE, you might encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than \*CHANGE, make sure that all device descriptions and their associated message queues have a PUBLIC authority of \*CHANGE. One way to accomplish this is to change the CRTAUT value for library QSYS to \*CHANGE from \*SYSVAL.

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaut\\_hnobj.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaut_hnobj.htm)

#### 4.1.1.12 (L1) Set Disconnect-Job Interval (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies the interval in minutes that a job can be disconnected before the system ends the job.

**Rationale:**

A disconnected job uses up system resources, as well as retaining any locks on objects and should be ended eventually to avoid this.

**Audit:**

DSPSYSVAL SYSVAL(QDSCJOBTV)

**Remediation:**

To establish the recommended configuration, set the following system value to "30" (Times out disconnected jobs after 30 minutes):

QDSCJOBTV

CHGSYSVAL SYSVAL(QDSCJOBTV) VALUE('30')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarldscjob.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarldscjob.htm)

#### *4.1.1.13 (L1) Set Display User Sign-on Information (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Specifies whether the sign-on information display appears when a user signs on. Promotes logon monitoring.

**Rationale:**

This is recommended so that users can monitor attempted use of their profiles.

**Audit:**

DSPSYSVAL SYSVAL(QDSPSGNINF)

**Remediation:**

To establish the recommended configuration, set the following system value to "1" (ON):

QDSPSGNINF

CHGSYSVAL SYSVAL(QDSPSGNINF) VALUE('1')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarldspi.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarldspi.htm)

#### 4.1.1.14 (L1) Set Force Conversion On Restore (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines under what conditions objects will be forced to convert when they are being restored to the system. When an object is translated it is recompiled using a trusted translator guaranteed not to circumvent the integrity of the system. (See also QALWOBJRST & QVFYOBJRST, 2.1.1.1 and 2.1.1.49)

**Rationale:**

This setting attempts to strike a balance between ensuring system integrity and incurring the overhead of recompiling programs that do not appear to have been altered.

**Audit:**

DSPSYSVAL SYSVAL(QFRCCVNRST)

**Remediation:**

To establish the recommended configuration, set the following system value to "3":

QFRCCVNRST

CHGSYSVAL SYSVAL(QFRCCVNRST) VALUE('3')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/ilec/sc41560666.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/ilec/sc41560666.htm)

#### 4.1.1.15 (L1) Set Inactivity Time-out Interval (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines the interval in minutes that a workstation can be inactive before the system sends a message to a message queue or ends the job. All users must use a password protected screen saver that locks the PC after 15 minutes of inactivity to comply with Payment Card Industry Data Security Standards.

**Rationale:**

The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed on. An inactive workstation might allow an unauthorized person access to the system.

**Audit:**

DSPSYSVAL SYSVAL(QINACTITV)

**Remediation:**

To establish the recommended configuration, set the following system value to "30" (The system times out inactive jobs after 30 minutes of inactivity):

QINACTITV

CHGSYSVAL SYSVAL(QINACTITV) VALUE('30')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarltminv.html](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarltminv.html)



#### 4.1.1.16 (L1) Set Inactivity Message Queue (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies either the action to be taken when the inactivity time-out interval is reached or the name of the message queue that will receive messages about the workstation. The current system standard ends the job after the inactivity time-out interval is reached.

**Rationale:**

Controlling inactive jobs provides security so that users do not leave signed on displays inactive.

**Audit:**

DSPSYSVAL SYSVAL(QINACTMSGQ)

**Remediation:**

To establish the recommended configuration, set the following system value to \*DSCJOB:  
QINACTMSGQ  
CHGSYSVAL SYSVAL(QINACTMSGQ) VALUE('\*DSCJOB')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarltmq.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarltmq.htm)

#### 4.1.1.17 (L1) Set Limit Device Sessions (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies if users can have concurrent device sessions.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QLMTDEVSSN)

**Remediation:**

To establish the recommended configuration, set the following system value to any value between 1 and 9:

QLMTDEVSSN

CHGSYSVAL SYSVAL(QLMTDEVSSN) VALUE(<x>)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarllmtdecsn.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarllmtdecsn.htm)

#### *4.1.1.18 (L1) Set Limit Security Officer Access to Workstations (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Limits users with \*ALLOBJ or \*SERVICE special authority to authorized devices.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QLMTSECOFR)

**Remediation:**

To establish the recommended configuration, set the following system value to "0":

QLMTSECOFR

CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('0')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarllmtso.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarllmtso.htm)

#### 4.1.1.19 (L1) Set Maximum Sign-on Action (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines the action the system takes when a user reaches the maximum number of sign-on attempts.

Disables the user profile when the maximum sign-on limit is reached.

**Rationale:**

This disables the user profile when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same or different devices. This helps to prevent access to unauthorized users.

**Audit:**

DSPSYSVAL SYSVAL(QMAXSGNACN)

**Remediation:**

To establish the recommended configuration, set the following system value to "2":

QMAXSGNACN

CHGSYSVAL SYSVAL(QMAXSGNACN) VALUE('2')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlacti on.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlacti on.htm)

#### *4.1.1.20 (L1) Set Maximum Sign-on Attempts (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Determines the maximum number of invalid sign-on attempts a user is allowed.

**Rationale:**

This setting helps to prevent unauthorized access into user profiles by giving the user a limited number of login attempts before disabling the user profile

**Audit:**

DSPSYSVAL SYSVAL(QMAXSIGN)

**Remediation:**

To establish the recommended configuration, set the following system value to "5":

QMAXSIGN

CHGSYSVAL SYSVAL(QMAXSIGN) VALUE('5')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlmaxsgn.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlmaxsgn.htm)

#### 4.1.1.21 (L1) Set Block Password Change (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Specifies the time period during which a password is blocked from being changed following the prior successful password change operation. This system value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command.

##### **Rationale:**

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

##### **Audit:**

DSPSYSVAL SYSVAL(QPWDCHGBLK)

##### **Remediation:**

To establish the recommended configuration, set the following system value to "24":

QPWDCHGBLK

CHGSYSVAL SYSVAL(QPWDCHGBLK) VALUE('24')

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpwdchgbk.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpwdchgbk.htm)

#### 4.1.1.22 (L1) Set Password Expiration Interval (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines the maximum number of days a password is valid from 1 to 366 or \*NOMAX. Note that special application profiles that must logon should have PWDEXPITV set to \*NOMAX on the user profile whereas standard user profiles should be set to \*SYSVAL.

**Rationale:**

This helps to prevent access to unauthorized persons by forcing a password change after a set amount of days.

**Audit:**

DSPSYSVAL SYSVAL(QPWDEXPITV)

**Remediation:**

To establish the recommended configuration, set the following system value to "90":

QPWDEXPITV

CHGSYSVAL SYSVAL(QPWDEXPITV) VALUE('90')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlexp.itv.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlexp.itv.htm)

#### *4.1.1.23 (L1) Set Password Expiration Warning (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Controls the number of days prior to a password expiring to begin displaying password expiration warning messages on the Sign-on Information display.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QPWDEXPWRN)

**Remediation:**

To establish the recommended configuration, set the following system value to "7":

QPWDEXPWRN

CHGSYSVAL SYSVAL(QPWDEXPWRN) VALUE('7')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpw\\_dexpwrn.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpw_dexpwrn.htm)



#### 4.1.1.24 (L1) Set Password Level (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Determines the length of password that is supported as well as weak and deprecated NTLM passwords for Windows 95/98/ME clients will be removed from the system. User passwords with a length of 1-10 characters are supported and excludes the use of decryptable password hashes (NTLM) for older 16 bit clients.

Note that NTLM or Lan Manager authentication uses a method of hashing a user's password into 14 (7+7) characters and the hash is calculated into the two halves separately making it easily decryptable. NTLM was replaced by NTLMv2 in the late 1990s and has since been deprecated.

##### **Rationale:**

This provides additional security by having options to only support passwords that meets specified length and security requirements.

##### **Audit:**

DSPSYSVAL SYSVAL(QPWDLVL)

##### **Remediation:**

To establish the recommended configuration, set the following system value to "1":

QPWDLVL

CHGSYSVAL SYSVAL(QPWDLVL) VALUE(1)

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlnewpwdlevels.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlnewpwdlevels.htm)

#### 4.1.1.25 (L1) Set Required Difference in Passwords (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies a code that determines how many of the most recent prior passwords are not allowed.

**Rationale:**

This value provides additional security by preventing users from specifying passwords that were used previously. It also prevents a user whose password has expired from changing it and then immediately changing it back to the old password.

**Audit:**

DSPSYSVAL SYSVAL(QPWDRQDDIF)

**Remediation:**

To establish the recommended configuration, set the following system value to "8":

QPWDRQDDIF

CHGSYSVAL SYSVAL(QPWDRQDDIF) VALUE('8')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlrqddif.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlrqddif.htm)

#### 4.1.1.26 (L1) Set Password Rules (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies the rules used to check whether a password is formed correctly.

**Rationale:**

This provides additional security by having a system in place to verify if a password meets the specified rules set.

**Audit:**

DSPSYSVAL SYSVAL(QPWDRULES)

**Remediation:**

- CALL QCMD
- CHGSYSVAL SYSVAL(QPWDRULES) VALUE('\*ALLCRTCHG \*DGTLMTAJC \*DGTLMTFST \*DGTLMTLST \*DGTMIN1 \*LMTPRFNAME \*MAXLEN10 \*MINLEN8 \*REQANY3 \*SPCCHRLMTAJC \*SPCCHRLMTFST \*SPCCHRLMTLST')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpwdrules.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpwdrules.htm)

#### 4.1.1.27 (L1) Retain Server Security (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines if the system will allow the storage of decryptable passwords to support connections to other systems from programs that must use an unencrypted password.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QRETSVRSEC)

**Remediation:**

To establish the recommended configuration, set the following system value to "1":

QRETSVRSEC

CHGSYSVAL SYSVAL(QRETSVRSEC) VALUE('1')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlretsvr.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlretsvr.htm)

#### 4.1.1.28 (L1) Set Remote IPL (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines if an operator is allowed to IPL the machine remotely.

**Rationale:**

Disabling this provides additional security by not allowing power-on and restart to be done remotely.

**Audit:**

DSPSYSVAL SYSVAL(QRMTIPL)

**Remediation:**

To establish the recommended configuration, set the following system value to "0":

QRMTIPL

CHGSYSVAL SYSVAL(QRMTIPL) VALUE('0')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqrmtipl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqrmtipl.htm)

#### 4.1.1.29 (L1) Set Remote Sign-on Value (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determine whether and how automatic sign-on from a remote system is allowed.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QRMTSIGN)

**Remediation:**

To establish the recommended configuration, set the following system value to \*VERIFY:

QRMTSIGN

CHGSYSVAL SYSVAL(QRMTSIGN) VALUE(\*VERIFY)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlrnctrl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlrnctrl.htm)

#### *4.1.1.30 (L1) Set Remote Service Attribute (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Determines if the remote system service ability is enabled.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QRMTSRVATR)

**Remediation:**

To establish the recommended configuration, set the following system value to "0":

QRMTSRVATR

CHGSYSVAL SYSVAL(QRMTSRVATR) VALUE('0')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlrmtsrv.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlrmtsrv.htm)

#### 4.1.1.31 (L1) Scan File System (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies the integrated file system in which objects will be scanned when exit programs are registered with any of the integrated file system scan-related exit points.

**Rationale:**

This provides an additional layer of security because this option can be used to scan for a virus.

**Audit:**

DSPSYSVAL SYSVAL(QSCANFS)

**Remediation:**

To establish the recommended configuration, set the following system value to

\*ROOTOPNUD:

QSCANFS

CHGSYSVAL SYSVAL(QSCANFS) VALUE('\*ROOTOPNUD')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqscanfs.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqscanfs.htm)



#### 4.1.1.32 (L1) Set Scan File System Control (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Controls the integrated file system scanning on the system when exit programs are registered with any of the integrated file system scan-related exit points.

**Rationale:**

This ensures that any failure from the scan exit programs prevent the associated operations, as well as not give the exit program additional access levels

**Audit:**

DSPSYSVAL SYSVAL(QSCANFCTL)

**Remediation:**

To establish the recommended configuration, set the following system value to \*ERRFAIL and \*NOWRTUPG:

QSCANFCTL

CHGSYSVAL SYSVAL(QSCANFCTL) VALUE(\*ERRFAIL \*NOWRTUPG')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqscanfctl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqscanfctl.htm)

#### 4.1.1.33 (L1) Set System Security Level (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Determines the level of security features supported. Level 40 is the recommended level of security for non-DoD production systems. In addition to password authentication and privileged access controls, level 40 can effectively safeguard data, programs, and other production objects and prevent unintentional data loss or modification. Level 50 can add considerable overhead depending on how the application is written and would need to be tested for performance impact before being implemented.

**Rationale:**

Security level 40 prevents potential integrity or security risks from programs that can circumvent security in special cases.

**Audit:**

DSPSYSVAL SYSVAL(QSECURITY)

**Remediation:**

To establish the recommended configuration, set the following system value to "40":

QSECURITY

CHGSYSVAL SYSVAL(QSECURITY) VALUE('40')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlseclvl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlseclvl.htm)

#### 4.1.1.34 (L1) Set Shared Memory Control (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Controls whether or not users are allowed to use shared memory APIs or mapped memory objects that have write capability to modify shared memory. While enabling this system value introduces the possibility of an integrity issue if not used correctly, the probability is low given our systems other security controls. Specifically, restricting the ability to create, restore, or use shared memory APIs.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QSHRMEMCTL)

**Remediation:**

To establish the recommended configuration, set the following value to "1":

QSHRMEMCTL

CHGSYSVAL SYSVAL(QSHRMEMCTL) VALUE('1')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlshrmemctl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlshrmemctl.htm)

#### 4.1.1.35 (L1) Secure Sockets Layer (SSL) cipher specification list (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Specifies the list of cipher suites that are supported by System SSL. The values are read-only unless the QSSLCSLCTL (SSL cipher control) system value is set to \*USRDFN.

##### **Rationale:**

Federal Information Processing Standards Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems.

##### **Audit:**

DSPSYSVAL QSSLCSL

##### **Remediation:**

Specify the following cipher suites that are supported by System SSL:

- CALL QCMD
- CHGSYSVAL SYSVAL(QSSLCSL) VALUE('\*ECDHE\_ECDSA\_AES\_256\_GCM\_SHA384 \*ECDHE\_ECDSA\_AES\_128\_GCM\_SHA256 \*ECDHE\_RSA\_AES\_256\_GCM\_SHA384 \*ECDHE\_RSA\_AES\_128\_GCM\_SHA256 \*RSA\_AES\_256\_GCM\_SHA384 \*RSA\_AES\_128\_GCM\_SHA256')

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqssl.html](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqssl.html)

#### 4.1.1.36 (L1) Set Transport Layer Security cipher control (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Specifies whether or not the QSSLCSL (SSL cipher specification list) system value is controlled by the system or by the user.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QSSLCSLCTL)

**Remediation:**

To establish the recommended configuration, set the following system value to \*USRDFN:

QSSLCSLCTL

CHGSYSVAL SYSVAL(QSSLCSLCTL) VALUE('\*USRDFN')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqsslctl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqsslctl.htm)

#### *4.1.1.37 (L1) Transport Layer Security protocols (Scored)*

**Profile Applicability:**

- Level 1

**Description:**

Specifies the SSL protocol versions supported by System SSL.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QSSLPCL)

**Remediation:**

To establish the recommended configuration, set the following system value to \*TLSV1.2:

QSSLPCL

CHGSYSVAL SYSVAL(QSSLPCL) VALUE(\*TLSV1.2')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqsslpcl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqsslpcl.htm)

### 4.1.1.38 (L1) System Library List (Scored)

#### Profile Applicability:

- Level 1

#### Description:

The system library list (QSYSLIBL) system value is used as the first part of the library list associated with a job.

The libraries in the system part of the library list of a job are searched before any other libraries in the library list of a job. The list can contain as many as 15 names. You cannot delete or rename a library specified as part of the system library list, because libraries in this library list are locked.

You can change the system library list (QSYSLIBL). If you change QSYSLIBL, the change takes place immediately for new jobs entering the system. The change does not affect running jobs, unless the application in the job accesses the system library list directly.

#### Rationale:

The security of the System Library List is a vital part of your overall system security. All libraries in the System Library List should provide \*PUBLIC \*USE authority. Any authority greater than \*USE to any library in the System Library List can allow the introduction of trojans and malicious code into your system that will be searched before any other libraries in the library list of a job.

#### Audit:

DSPPSYVAL SYSVAL(QSYSLIBL)

- Make note of all Libraries in the System part of the library list
- DSPOBJAUT OBJ(<xxxxxx>) OBJTYPE(\*LIB) For each library in the list
- Ensure that each library in the list grants \*PUBLIC \*USE Object Authority and that any additional Users with an authority greater than \*USE are properly authorized by the business to introduce changes into the library.

#### Remediation:

To establish the recommended configuration, set the \*PUBLIC authority to \*USE to all libraries in the System part of the library list QSYSLIBL that grant an authority greater than \*USE:

GRTOBJAUT OBJ(<xxxxxx>) OBJTYPE(\*LIB) USER(\*PUBLIC) AUT(\*USE) REPLACE(\*YES)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/nls/rbagsqsyslibluse.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/nls/rbagsqsyslibluse.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rbam6/jlibl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rbam6/jlibl.htm)



#### 4.1.1.39 (L1) Set Use Adopted Authority (Scored) (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Controls those users allowed to create or change programs that use adopted authority from other programs that call it. If an authorization list is specified, \*PUBLIC(EXCLUDE) should be used. Specific access granted for those users that are allowed to create or change programs that adopt authority should be limited to system administrator personnel and change control personnel responsible for disaster recovery and program change control respectively.

##### **Rationale:**

##### **Audit:**

DSPSYSVAL SYSVAL(QUSEADPAUT)

##### **Remediation:**

To establish the recommended configuration, enter a name for the authorization list for the following system value:

QUSEADPAUT

- CRTAUTL AUTL(QUSEADPAUT) AUT(\*EXCLUDE)
- CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(\*AUTL) NEWOWN(QSYS)
- CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/ilec/uadpaut.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/ilec/uadpaut.htm)

#### 4.1.1.40 (L1) Verify Object On Restore (Scored) (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

Determines when signatures will be verified and if the object will be restored without a valid signature. (See also QALWOBJRST & QFRCCVNRST, 2.1.1.1 and 2.1.1.16) Use this value for normal operations, when you expect some of the objects you restore to be unsigned, but you want to ensure that all signed objects have signatures that are valid. Commands and programs you have created or purchased before digital signatures were available will be unsigned. This value allows those commands and programs to be restored. This is the default value.

##### **Rationale:**

You can prevent anyone from restoring an object, unless that object has a correct digital signature from a trusted software provider.

##### **Audit:**

DSPSYSVAL SYSVAL(QVIFYOBJRST)

##### **Remediation:**

To establish the recommended configuration, set the following system value to "3":

QVIFYOBJRST

CHGSYSVAL SYSVAL(QVIFYOBJRST) VALUE('3')

##### **Impact:**

When your system is shipped, the QVIFYOBJRST system value is set to 3. If you change the value of QVIFYOBJRST, it is important to set the QVIFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarm/rzarmq\\_vfyobjrstsysval.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarm/rzarmq_vfyobjrstsysval.htm)

## 4.1.2 Level 2

High Security/Sensitive Data Environment (limited functionality)

### 4.1.2.1 (L2) Allow Restoration of Security-Sensitive Objects (Scored)

#### Profile Applicability:

- Level 2

#### Description:

Does not allow objects with security-sensitive attributes to be restored.

#### Rationale:

Because some programs may cause serious problems, this system value provides a method to protect your system.

#### Audit:

DSPSYSVAL SYSVAL(QALWOBJRST)

#### Remediation:

To establish the recommended configuration, set the following system value to \*NONE:

QALWOBJRST

CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('\*NONE')

#### Impact:

It is important to set the QALWOBJRST value to \*ALL before performing some system activities, such as:

- Installing a new release of the IBM® i licensed program
- Installing new licensed programs
- Recovering your system

These activities may fail if the QALWOBJRST value is not \*ALL. To ensure system security, return the QALWOBJRST value to your normal setting after completing the system activity.

#### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlqalwrst.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlqalwrst.htm)

#### 4.1.2.2 (L2) Allow User Domain Objects in These Libraries (Scored)

##### **Profile Applicability:**

- Level 2

##### **Description:**

This specifies the names of the libraries that can contain the \*USRSPC (user space), \*USRIDX (user index), and \*USRQ (user queue) type objects. In our environment many vendor applications are making use of USRxx objects in numerous and changing libraries. This increases the complexity of restricting this system value to specific libraries without creating a threat to legitimate operations.

In addition, the value of \*ALL is generally acceptable for any system that does not need to comply with DoD C2 level security specifications. In addition, the probability of damaging events is low if object authority and application behavior is controlled appropriately. This is the shipped value.

##### **Rationale:**

Some systems have application software that relies on object types \*USRSPC, \*USRIDX, or \*USRQ. For those systems, the list of libraries for the QALWUSRDMN system value should include the libraries that are used by the application software.

##### **Audit:**

```
DSPSYSVAL SYSVAL(QALWUSRDMN)
```

##### **Remediation:**

To establish the recommended configuration, set the following system value to QTEMP:

```
QALWUSRDMN
```

```
CHGSYSVAL SYSVAL(QALWUSRDMN) VALUE('QTEMP')
```

##### **Impact:**

Systems with high security requirements require the restriction of user \*USRSPC, \*USRIDX, \*USRQ objects. The system cannot audit the movement of information to and from user domain objects. The restriction does not apply to user domain objects of type program (\*PGM), server program (\*SRVPGM), and SQL packages (\*SQLPKG).

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzar1/rzar1qalwusr.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzar1/rzar1qalwusr.htm)

**Notes:**

If your system has a high security requirement, you should allow user domain objects only in the QTEMP library

### 4.1.2.3 (L2) Set Auditing Control (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Serves as the on/off switch for security auditing. \*AUDLVL activates event auditing at the system or user level. \*OBJAUD activates object auditing. \*NOQTEMP prevents extraneous auditing entries for objects in library QTEMP.

**Rationale:**

Auditing can be defined as an inspection or examination of a process or system to determine the quality of it, and is also used to ensure compliance to requirements.

Activates event and object auditing including QTEMP

**Audit:**

DSPSYSVAL SYSVAL(QAUDCTL)

**Remediation:**

To establish the recommended configuration, set the following system value to \*OBJAUD, \*AUDLVL :

QAUDCTL

CHGSYSVAL SYSVAL(QAUDCTL) VALUE('\*OBJAUD \*AUDLVL')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaudcon.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaudcon.htm)

#### 4.1.2.4 (L2) Set Auditing End Action (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the action the system should take if it is unable to continue auditing (e.g. the audit record is full).

**Rationale:**

If the system is unable to write audit journal entries and the QAUDENDACN system value is \*PWRDWNSYS, your system ends abnormally. This might cause a lengthy initial program load (IPL) when your system is powered on again.

**Audit:**

DSPSYSVAL SYSVAL(QAUDENDACN)

**Remediation:**

To establish the recommended configuration, set the following system value to

\*PWRDWNSYS:

QAUDENDACN

CHGSYSVAL SYSVAL(QAUDENDACN) VALUE('\*PWRDWNSYS')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlauditea.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlauditea.htm)

#### 4.1.2.5 (L2) Set Auditing Force Level (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines how many auditing journal entries records are cached in memory before they are physically written to disk from memory.

**Rationale:**

This will provide the best auditing performance.

**Audit:**

DSPSYSVAL SYSVAL(QAUDFRCLVL)

**Remediation:**

To establish the recommended configuration, set the following system value to "1":

QAUDFRCLVL

CHGSYSVAL SYSVAL(QAUDFRCLVL) VALUE(1)

**Impact:**

if your installation requires that no audit entries be lost when your system ends abnormally, you must specify 1. Specifying 1 might impair performance.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlauditfl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlauditfl.htm)



#### 4.1.2.6 (L2) Set Automatic Virtual Device Creation (Scored)

##### **Profile Applicability:**

- Level 2

##### **Description:**

Determines whether automatic device creation is allowed and if so, how many devices can be configured automatically. 32500 is the maximum numerical value that can be set for this system value and is both sufficient to support the needs of the business and not too large to represent a denial of service exposure since it represents a finite limit.

##### **Rationale:**

Prevents new virtual devices from being created.

##### **Audit:**

DSPSYSVAL SYSVAL(QAUTOVRT)

##### **Remediation:**

To establish the recommended configuration, set the following system value to "0":

QAUTOVRT

CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(0)

##### **Impact:**

Users are able to break into your system more easily using pass-through or telnet if you allow the system to automatically configure virtual devices. A user that is attempting to break in has a limited number of attempts at each virtual device without automatic configuration.

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlautovrt.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlautovrt.htm)

#### 4.1.2.7 (L2) Set Create Authority (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies the default public authority.

Sets \*EXCLUDE as the default public authority for new objects created in libraries that do not have a CRTAUT value specified.

**Rationale:**

This excludes the public from newly created objects. This will ensure the integrity of the newly created objects. You can override the QCRTAUT system value at a library level to specify data classifications within specific application libraries.

**Audit:**

DSPSYSVAL SYSVAL(QCRTAUT)

**Remediation:**

To establish the recommended configuration, set the following system value to \*EXCLUDE:  
QCRTAUT  
CHGSYSVAL SYSVAL(QCRTAUT) VALUE(\*EXCLUDE')

**Impact:**

Several IBM-supplied libraries, including QSYS, have a CRTAUT value of \*SYSVAL. If you change the QCRTAUT system value to something other than \*CHANGE, you might encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than \*CHANGE, make sure that all device descriptions and their associated message queues have a PUBLIC authority of \*CHANGE. One way to accomplish this is to change the CRTAUT value for library QSYS to \*CHANGE from \*SYSVAL.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaut\\_hnobj.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaut_hnobj.htm)

#### 4.1.2.8 (L2) Set Create Object Audit Level (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the default object auditing level for new objects.

An audit record is written for any security relevant action that affects the read or change of all newly created objects.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QCRTOBJAUD)

**Remediation:**

To establish the recommended configuration, set the following system value to \*ALL:

QCRTOBJAUD

CHGSYSVAL SYSVAL(QCRTOBJAUD) VALUE('\*ALL')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlaudnobj.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlaudnobj.htm)

#### 4.1.2.9 (L2) Set Disconnect-Job Interval (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies the interval in minutes that a job can be disconnected before the system ends the job.

**Rationale:**

A disconnected job uses up system resources, as well as retaining any locks on objects and should be ended eventually to avoid this.

**Audit:**

DSPSYSVAL SYSVAL(QDSCJOBTV)

**Remediation:**

To establish the recommended configuration, set the following system value to "15" (Times out disconnected jobs after 15 minutes):

QDSCJOBTV

CHGSYSVAL SYSVAL(QDSCJOBTV) VALUE('15')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarldscjob.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarldscjob.htm)

#### 4.1.2.10 (L2) Set Force Conversion On Restore (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines under what conditions objects will be forced to convert when they are being restored to the system. When an object is translated it is recompiled using a trusted translator guaranteed not to circumvent the integrity of the system. (See also QALWOBJRST & QVFYOBJRST, 2.1.2.1 and 2.1.2.31)

All objects will be converted.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QFRCCVNRST)

**Remediation:**

To establish the recommended configuration, set the following system value to "7":

QFRCCVNRST

CHGSYSVAL SYSVAL(QFRCCVNRST) VALUE('7')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/ilec/sc41560666.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/ilec/sc41560666.htm)

#### 4.1.2.11 (L2) Set Inactivity Time-out Interval (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the interval in minutes that a workstation can be inactive before the system sends a message to a message queue or ends the job. All users must use a password protected screen saver that locks the PC after 15 minutes of inactivity to comply with Payment Card Industry Data Security Standards.

**Rationale:**

The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed on. An inactive workstation might allow an unauthorized person access to the system.

**Audit:**

DSPSYSVAL SYSVAL(QINACTITV)

**Remediation:**

To establish the recommended configuration, set the following system value to "15" (The system times out inactive jobs after 15 minutes of inactivity):

QINACTITV

CHGSYSVAL SYSVAL(QINACTITV) VALUE('15')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarltmintrl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarltmintrl.htm)

#### 4.1.2.12 (L2) Set Inactivity Message Queue (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies either the action to be taken when the inactivity time-out interval is reached or the name of the message queue that will receive messages about the workstation. The current system standard ends the job after the inactivity time-out interval is reached.

**Rationale:**

Controlling inactive jobs provides security so that users do not leave signed on displays inactive.

**Audit:**

DSPSYSVAL SYSVAL(QINACTMSGQ)

**Remediation:**

To establish the recommended configuration, set the following system value to \*ENDJOB:  
QINACTMSGQ  
CHGSYSVAL SYSVAL(QINACTMSGQ) VALUE('\*ENDJOB')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarltmq.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarltmq.htm)

#### 4.1.2.13 (L2) Set Limit Device Sessions (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies if users can have concurrent device sessions.

**Rationale:**

This is recommended because limiting users to a single device reduces the likelihood of sharing passwords and leaving devices unattended.

**Audit:**

DSPSYSVAL SYSVAL(QLMTDEVSSN)

**Remediation:**

To establish the recommended configuration, set the following system value to '1':

QLMTDEVSSN

CHGSYSVAL SYSVAL(QLMTDEVSSN) VALUE('1')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarllmtdecsn.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarllmtdecsn.htm)



#### 4.1.2.14 (L2) Set Limit Security Officer Access to Workstations (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Limits users with \*ALLOBJ or \*SERVICE special authority to authorized devices.

**Rationale:**

This system value controls whether users with \*ALLOBJ or \*SERVICE special authorities need explicit authority to specific work stations.

**Audit:**

DSPSYSVAL SYSVAL(QLMTSECOFR)

**Remediation:**

To establish the recommended configuration, set the following system value to "1":

QLMTSECOFR

CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('1')

**Impact:**

If the value of QLMTSECOFR is set to a value of 1, a user with \*ALLOBJ or \*SERVICE special authority can sign on at a workstation only if that user is specifically authorized (that is, given \*CHANGE authority) to the workstation or if user profile QSECOFR is authorized (given \*CHANGE authority) to the workstation. This authority cannot come from public authority.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarllmtso.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarllmtso.htm)

#### 4.1.2.15 (L2) Set Maximum Sign-on Action (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the action the system takes when a user reaches the maximum number of sign-on attempts.

Disables the user profile and device when the maximum sign-on limit is reached.

**Rationale:**

This disables the user profile when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same or different devices. This helps to prevent access to unauthorized users.

**Audit:**

DSPSYSVAL SYSVAL(QMAXSGNACN)

**Remediation:**

To establish the recommended configuration, set the following system value to "3":

QMAXSGNACN

CHGSYSVAL SYSVAL(QMAXSGNACN) VALUE('3')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlacti on.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlacti on.htm)

#### 4.1.2.16 (L2) Set Maximum Sign-on Attempts (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the maximum number of invalid sign-on attempts a user is allowed.

**Rationale:**

This setting helps to prevent unauthorized access into user profiles by giving the user a limited number of login attempts before disabling the user profile

**Audit:**

DSPSYSVAL SYSVAL(QMAXSIGN)

**Remediation:**

To establish the recommended configuration, set the following system value to "3":

QMAXSIGN

CHGSYSVAL SYSVAL(QMAXSIGN) VALUE('3')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlmaxsgn.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlmaxsgn.htm)

#### 4.1.2.17 (L2) Set Block Password Change (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies the time period during which a password is blocked from being changed following the prior successful password change operation. This system value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command.

**Rationale:**

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

**Audit:**

DSPSYSVAL SYSVAL(QPWDCHGBLK)

**Remediation:**

To establish the recommended configuration, set the following system value to "99":

QPWDCHGBLK

CHGSYSVAL SYSVAL(QPWDCHGBLK) VALUE('99')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpwdchgbk.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpwdchgbk.htm)

#### 4.1.2.18 (L2) Set Password Level (Scored)

##### **Profile Applicability:**

- Level 2

##### **Description:**

Determines the length of password that is supported as well as weak and deprecated NTLM passwords for Windows 95/98/ME clients will be removed from the system. User passwords with a length of 1-128 characters are supported and excludes the use of decryptable password hashes (NTLM) for older 16 bit clients.

Note that NTLM or Lan Manager authentication uses a method of hashing a user's password into 14 (7+7) characters and the hash is calculated into the two halves separately making it easily decryptable. NTLM was replaced by NTLMv2 in the late 1990s and has since been deprecated.

##### **Rationale:**

This provides additional security by having options to only support passwords that meets specified length and security requirements.

##### **Audit:**

DSPPSYVAL SYSVAL(QPWDLVL)

##### **Remediation:**

To establish the recommended configuration, set the following system value to "3":

QPWDLVL

CHGSYSVAL SYSVAL(QPWDLVL) VALUE(3)

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlnewpwdlevels.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlnewpwdlevels.htm)

##### **Notes:**

Note: When the current or pending value of the password level (QPWDLVL) system value is 2 or 3, a program name cannot be specified for the Password Approval Program system value QPWDVLDPGM. Therefore, at QPWDLVL = 3, system value QPWDVLDPGM should be set to a value of \*REGFAC or \*NONE.

#### 4.1.2.19 (L2) Set Required Difference in Passwords (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies a code that determines how many of the most recent prior passwords are not allowed.

**Rationale:**

This value provides additional security by preventing users from specifying passwords that were used previously. It also prevents a user whose password has expired from changing it and then immediately changing it back to the old password.

**Audit:**

DSPSYSVAL SYSVAL(QPWDRQDDIF)

**Remediation:**

To establish the recommended configuration, set the following system value to "1":

QPWDRQDDIF

CHGSYSVAL SYSVAL(QPWDRQDDIF) VALUE('1')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlrqddif.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlrqddif.htm)

#### 4.1.2.20 (L2) Set Password Rules (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Specifies the rules used to check whether a password is formed correctly.

**Rationale:**

This provides additional security by having a system in place to verify if a password meets the specified rules set.

**Audit:**

DSPSYSVAL SYSVAL(QPWDRULES)

**Remediation:**

- CALL QCMD
- CHGSYSVAL SYSVAL(QPWDRULES) VALUE('\*ALLCRTCHG \*DGTLMTAJC \*DGTLMTFST \*DGTLMTLST \*DGTMIN1 \*LMTPRFNAME \*MAXLEN128 \*MINLEN14 \*REQANY3 \*SPCCHRLMTAJC \*SPCCHRLMTFST \*SPCCHRLMTLST')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpwdrules.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpwdrules.htm)

#### 4.1.2.21 (L2) Set Password Validation Program (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:**

This provides the ability for a user-written program to do additional validation on passwords.

**Rationale:**

This provides additional security by using the programs to do additional checking of user-assigned passwords before they are accepted by the system.

**Audit:**

DSPSYSVAL SYSVAL(QPWDVLDPGM)

**Remediation:**

To establish the recommended configuration, create a password validation program and set the following system value to \*REGFAC:

QPWDVLDPGM

CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(\*REGFAC)

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlpw\\_dvldpgm.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlpw_dvldpgm.htm)

**Notes:**

Note: When the current or pending value of the password level (QPWDLVL) system value is 2 or 3, a program name cannot be specified for the Password Approval Program system value QPWDVLDPGM. Therefore, at QPWDLVL = 3, system value QPWDVLDPGM should be set to a value of \*REGFAC or \*NONE.



#### 4.1.2.22 (L2) Set Remote Sign-on Value (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determine whether and how automatic sign-on from a remote system is allowed.

**Rationale:****Audit:**

```
DSPSYSVAL SYSVAL(QRMTSIGN)
```

**Remediation:**

To establish the recommended configuration, set the following system value to

\*FRCSIGNON:

```
QRMTSIGN
```

```
CHGSYSVAL SYSVAL(QRMTSIGN) VALUE('*FRCSIGNON')
```

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlrnctrl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlrnctrl.htm)

#### 4.1.2.23 (L2) Retain Server Security (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines if the system will allow the storage of decryptable passwords to support connections to other systems from programs that must use an unencrypted password.

**Rationale:****Audit:**

DSPSYSVAL SYSVAL(QRETSVRSEC)

**Remediation:**

To establish the recommended configuration, set the following system value to "0":

QRETSVRSEC

CHGSYSVAL SYSVAL(QRETSVRSEC) VALUE('0')

**Impact:**

Setting QRETSVRSEC to a value of 0 prevents the storage of decryptable authentication information associated with DDM/DRDA Server Authentication Lists, Validation Lists (\*VLDL) and other types of decryptable authentication storage. This does not include the IBM i user profile password.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlretrvr.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlretrvr.htm)

#### 4.1.2.24 (L2) Set System Security Level (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines the level of security features supported. Level 40 is the recommended level of security for non-DoD production systems. In addition to password authentication and privileged access controls, level 40 can effectively safeguard data, programs, and other production objects and prevent unintentional data loss or modification. Level 50 can add considerable overhead depending on how the application is written and would need to be tested for performance impact before being implemented.

**Rationale:**

Security level 50 provides enhanced integrity protection, in addition to what is provided by security level 40, for installations with strict security requirements.

**Audit:**

DSPSYSVAL SYSVAL(QSECURITY)

**Remediation:**

To establish the recommended configuration, set the following system value to "50":

QSECURITY

CHGSYSVAL SYSVAL(QSECURITY) VALUE('50')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlseclvl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlseclvl.htm)

#### 4.1.2.25 (L2) Set Shared Memory Control (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:****Rationale:****Audit:**

DSPSYSVAL SYSVAL(QSHRMEMCTL)

**Remediation:**

To establish the recommended configuration, set the following value to "0":

QSHRMEMCTL

CHGSYSVAL SYSVAL(QSHRMEMCTL) VALUE('0')

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlshrmemctl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlshrmemctl.htm)

#### 4.1.2.26 (L2) Verify Object On Restore (Scored) (Scored)

**Profile Applicability:**

- Level 2

**Description:**

Determines when signatures will be verified and if the object will be restored without a valid signature. (See also QALWOBJRST & QFRCCVNRST, 2.1.2.1 and 2.1.2.10)

**Rationale:**

You can prevent anyone from restoring an object, unless that object has a correct digital signature from a trusted software provider.

**Audit:**

DSPSYSVAL SYSVAL(QVIFYOBJRST)

**Remediation:**

To establish the recommended configuration, set the following system value to "5":

QVIFYOBJRST

CHGSYSVAL SYSVAL(QVIFYOBJRST) VALUE('5')

**Impact:**

When your system is shipped, the QVIFYOBJRST system value is set to 3. If you change the value of QVIFYOBJRST, it is important to set the QVIFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarlvfyobj.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarlvfyobj.htm)

## 4.2 Network Services

Access to the \*IOSYSCFG special authority must be limited to only those individuals responsible for configuring lines, controllers, and devices to limit changes to the system network configuration. Access to the \*ALLOBJ and \*SECADM special authority must be limited to those who need access. Access to both of these privileges is required to change the following network security attributes using the CHGNETA command. All changes must be documented and approved.

### 4.2.1 (L1) Network Attribute JOBACN (Network Job Action) (Scored)

#### Profile Applicability:

- Level 1

#### Description:

Specifies the action taken for input streams received through the SNA network by the system. The JOBACN value should be set to \*REJECT to secure your system from job streams received through the network.

#### Rationale:

The Job Action setting controls remote request to run local jobs. The default setting is \*FILE which files remote input streams on the queue for the receiving user who can then display, cancel, or receive the input allowing potentially unwanted remote commands to run on the local system. The recommended value is \*REJECT which will send both the sender and receiver a message stating that the input stream was rejected.

#### Audit:

- DSPNETA
- Page Down and verify that the value for Job action is set to \*REJECT.

#### Remediation:

To establish the recommended configuration, change the Network Attribute JOBACN to \*REJECT:

```
CHGNETA JOBACN (*REJECT)
```

#### Impact:

Changing Network Attribute JOBACN to \*REJECT may disable SNA network job streams from entering your system without proper credentialed authentication.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzarl/rzarljobact.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzarl/rzarljobact.htm)

## 4.2.2 (L1) DDM Remote Configuration List (SNA) Attributes (Scored)

### Profile Applicability:

- Level 1

### Description:

All DDM Remote Configuration List entries shall specify \*VFYENCPWD for the Secure Location (SECURELOC) parameter. \*VFYENCPWD requires the same user ID and password on each source and target system.

To avoid having to use shared default user profiles, create a user profile on each system where the user needs access to the distributed relational database.

### Rationale:

Setting the Secure Loc Parameter of all remote locations ensures that encrypted password are required for SNA DDM/DRDA communications.

### Audit:

- DSPCFGL CFGL(QAPPNRMT)  
-Note that if you receive the message “Configuration list QAPPNRMT not found”, this indicates that your system does is not configured for DDM over SNA and this setting is irrelevant.
- Ensure that all Secure Loc parameters = \*VFYENCPWD.

### Remediation:

To establish the recommended configuration, change all Remote Location Secure Loc parameters to \*VFYENCPWD.

WRKCFGL CFGL(QAPPNRMT)

Select 2 to change the QAPPNRMT Configuration List

Change all Secure Loc parameters to \*VFYENCPWD

### Impact:

Shared (non-unique) accounts in an APPN network may be impacted.

### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/ddp/rbal1tsse.c.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/ddp/rbal1tsse.c.htm)



### 4.2.3 (L1) DDM TCP/IP Attributes (Scored)

#### Profile Applicability:

- Level 1

#### Description:

The default setting for the DDM server has a default security of \*USRIDPWD which allows clear-text password.

#### Rationale:

Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources. Additionally, a setting lower than \*USRIDPWD such as \*YES, \*VLDONLY or \*USRID does not require a password on a DDM Connection request allowing un-authenticated access to system resources possibly with elevated privileges.

#### Audit:

Type CHGDDMTCPA and press F4.

The screen will display the DDM TCP/IP Attributes. Ensure that the Lowest authentication method equals \*USRENCPWD and the Lowest encryption algorithm is equal to \*AES.

#### Remediation:

To establish the recommended configuration, change all non-administrative \*USER class users and groups to SPCAUT = \*NONE:

```
CHGDDMTCPA AUTOSTART(*YES) PWDRQD(*USRENCPWD) ENCALG(*AES)
```

#### Impact:

DDM/DRDA communications not using encrypted passwords may be impacted.

#### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/ddp/rbal1elementsusetcp.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/ddp/rbal1elementsusetcp.htm)

#### 4.2.4 (L1) Telnet Protocol (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Restrict Telnet to SSL only to prevent sniffing of clear text passwords.

**Rationale:**

Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources.

**Audit:**

Type command CHGTelNA and press F4.

Ensure that the Allow Secure Socket Layer is set to \*ONLY.

**Remediation:**

To establish the recommended configuration, change telnet to use SSL only:

CHGTelNA ALWSSL(\*ONLY)

**Impact:**

Unencrypted telnet may be impacted.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamv/rzamvtcpsockets.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamv/rzamvtcpsockets.htm)

### 4.2.5 (L1) FTP Protocol (Scored)

**Profile Applicability:**

- Level 1

**Description:**

Restrict FTP to SSL only to prevent sniffing of clear text passwords.

**Rationale:**

Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources.

**Audit:**

Type command CHGFTPA and press F4.

Ensure that the Allow Secure Socket Layer is set to \*ONLY.

**Remediation:**

To establish the recommended configuration, change FTP to use SSL only:

```
CHGFTPA ALWSSL (*ONLY)
```

**Impact:**

Unencrypted ftp may be impacted.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamv/rzamvtcpsockets.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamv/rzamvtcpsockets.htm)

## 4.3 IBM i Netserver security

IBM i Support for Windows Network Neighborhood (IBM i NetServer) is an IBM i function that enables Windows 2000, Windows XP, Windows Server 2003, and Windows Vista clients to access IBM i shared directory paths and shared output queues.

By using IBM i NetServer securely, you can ensure that only authorized users can access IBM i NetServer resources, configuration, or shared data.

This section contains settings for configuring IBM i NetServer security settings using the IBM i Go Nets Menu. The IBM i Go Nets Menu is not enabled by default. Instructions for enabling the IBM i Go Nets Menu is available from IBM at [this link](#).

### 4.3.1 (L1) IBM i NetServer Guest Profile (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This policy setting determines whether a Guest account is configured. The Guest account allows unauthenticated network users to gain access to the system.

The recommended state for this setting is: \*NONE.

#### **Rationale:**

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

#### **Audit:**

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Guest profile \*NONE is displayed
- Ensure that \*SAME is displayed for the Guest profile Pending value to ensure no changes are pending.

**Remediation:**

To establish the recommended configuration, do the following:

- Type ADDLIBLE NETSRVCMD
- Type CHGNSVA GUESTPRF(\*NONE)
- Type ENDNSV
- Type STRNSV RESET(\*YES)

**Impact:**

Setting the IBM i NetServer Guest profile to a value of \*NONE may impact users access NetServer resources with a shared Guest profile. Additionally, changing the IBM i NetServer Guest profile requires you to end IBM i NetServer access (ENDNSV) and restart IBM I NetServer access (STRNSV RESET(\*YES) which may impact active sessions.

### 4.3.2 (L1) IBM i NetServer LANMAN Password Hash (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This policy specifies how clients will authenticate and prevents the use of insecure LANMAN password authentication. Because attackers can crack weak passwords, the stronger the password hash is, the more difficult the password is to crack.

#### **Rationale:**

The original LAN Manager password was developed in 1987. The LM hash is not a true one-way function as the passwords can be determined from the hash because of several weaknesses in its design. The original LM hash was replaced by the NTLMv1 protocol in 1993 and later updated in NTLMv2. Due to the multiple weaknesses in the LANMAN password, it has been deprecated and should no longer be used.

#### **Audit:**

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that LANMAN option \*NO is displayed
- Ensure that \*SAME is displayed for the LANMAN option Pending value to ensure no changes are pending.

#### **Remediation:**

To establish the recommended configuration, do the following:

- Type ADDLIBL NETSRVCMD
- Type CHGNSVA LANMANOPT(\*NO)
- Type ENDNSV
- Type STRNSV RESET(\*YES)

#### **Impact:**

Setting the IBM i NetServer LANMAN option to a value of \*NO may impact legacy authentication protocols in Windows 95/98. Additionally, changing the IBM i NetServer LANMAN option requires you to end IBM i NetServer access (ENDNSV) and restart IBM I NetServer access (STRNSV RESET(\*YES) which may impact active sessions.

### 4.3.3 (L1) IBM i SMB Signing (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This policy setting determines whether packet signing is required by the SMB client component.

#### **Rationale:**

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

#### **Audit:**

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Message authentication \*REQUIRED is displayed
- Ensure that \*SAME is displayed for the Message authentication Pending value to ensure no changes are pending.

#### **Remediation:**

To establish the recommended configuration, do the following:

- Type ADDLIBL NETSRVCMD
- Type CHGNSVA MSGAUT(\*REQUIRED)
- Type ENDNSV
- Type STRNSV RESET(\*YES)

#### **Impact:**

The network client will not communicate with a network server unless that server agrees to perform SMB packet signing.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

**Notes:**

When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.

The recommended state for this setting is: Enabled.



#### 4.3.4 (L1) IBM i SMBv2 Server (Scored)

##### Profile Applicability:

- Level 1

##### Description:

This setting configures the server-side processing of the Server Message Block version 2 (SMBv2) protocol.

##### Rationale:

Since September 2016, vendors have strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks than much newer designs such as SMBv2 and SMBv3.

##### Audit:

You can control which version(s) of SMB the NetServer will support by calling the NetServer maintenance utility to set the SMB flags and then restart the NetServer.

A good starting point is to see what those flags are presently set to.

In order to view the SMB flags do the following:

- CALL QZLSMAINT PARM('40' '0')
- Type WRKSPLF and locate your spool file with the name QPCSMPT. Verify that the data in the flags is as follows which indicates that the server supports only SMBv2:  
OLD FLAGS  
0000000000000500  
NEW FLAGS  
0000000000000500
- If the data for OLD FLAGS and NEW FLAGS is all 0s as shown below, this indicates that NetServer is using the default SMB version for your operating system version. At V7R2, that means that SMB version 1 (SMBv1) is being used exclusively with no support for SMBv2.  
OLD FLAGS  
0000000000000000  
NEW FLAGS  
0000000000000000

To recap, the SMB version support and the corresponding flag values for IBM i 7.2:

SMB1 only: 000

SMB1 & SMB2: 400

SMB2 only: 500

Setting the flags to any other value may have unpredictable results

### **Remediation:**

To allow SMB2 only, set the flags to a value of 500.

- `CALL QZLSMAINT PARM('40' '1' '0X500')`

Note that the flag values for 7.3 and beyond are different and the upgrade from 7.2 will not convert the SMB flags to the equivalent value for the new release so you will need to revisit these flags after an upgrade. This document explains how the flags are set for 7.3 [SMB and SMB2 Support for IBM i 7.3](#)

### **Impact:**

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: [SMB1 Product Clearinghouse | Storage at Microsoft](#)

### **References:**

1. <https://www.ibm.com/support/pages/smb2-support-ibm-i-72>

### 4.3.5 (L1) IBM i NetServer Shares (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This policy setting defines the network file shares available to authenticated users.

#### **Rationale:**

Allowing an IBM i NetServer File Shares allows authenticated users to access Server Message Block (SMB) file shares on the system.

Allowing users access to IBM I NetServer File shares grants authenticated users access to Integrated File System (IFS) directories. Use [this link](#) to learn more about the IFS. A file share to the root ('/') of the IBM I file system is never recommended to be configured as this would effectively give an attacker access to the root and all directories including qsys.lib (the operating system).

Additionally, pay careful attention to your existing share permissions. It is highly recommended to limit shares to Read only to prevent alteration of contents and protect from increasingly harmful crypto/ransomware attacks which detect network shares and may indiscriminately encrypt ubiquitous file systems of all types including qsys.lib. Use Read/Write permissions with diligence according to business requirements.

#### **Audit:**

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select Option 11. Work with Shares
- Place a 5 by each Share Name and observe the path of each share to ensure it is allowed by the business.
- Pay careful attention to ensure that no share allows access to the root (path /)

#### **Remediation:**

To establish the recommended configuration, do the following:

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select option 4 to remove the root (/) file share if detected

**Impact:**

Removing the root (/) file share will limit users to specific shares configured and prevent access to the root (/).

### 4.3.6 (L2) NetServer Browse Interval (Scored)

#### Profile Applicability:

- Level 2

#### Description:

Browse Announcements specify whether the server should announce its presence to the network.

#### Rationale:

For an added measure of security, you can hide IBM i NetServer from the Windows My Network Places.

#### Audit:

- Type ADDLIBL NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Browse interval is 0 is displayed
- Ensure that 0 is displayed for the Browse interval Pending value to ensure no changes are pending.

#### Remediation:

To establish the recommended configuration, do the following:

- Type ADDLIBL NETSRVCMD
- Type CHGNSVA BROWSEITV(\*NONE)
- Type ENDNSV
- Type STRNSV RESET(\*YES)

#### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzahl/rzahlhidenetserver.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzahl/rzahlhidenetserver.htm)

## 4.4 IBM i SSH Server security

The use of SSH provides a secure and encrypted mechanism for connecting to an IBM i server.

This section of the benchmark will focus on the installation and configuration of SSH. Some of the parameters specified in this section are actually the default values, but explicit declaration is preferred, to ensure that these recommendations remain constant over time.

Note: The SSH product directory is different between IBM i V7R2 and previous versions. After upgrading to V7R2, it is recommended that you migrate all settings to the V7R2 directory /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc and remove the older SSH product directories.

Remove the older product directories to prevent insecure settings from these directories from being used:

V5R4 - /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc

V6R1 - /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.8.1p1/etc/

V7R1 - /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-4.7p1/etc/

### 4.4.1 (L1) Configuring SSH – server protocol 2 (Scored)

#### Profile Applicability:

- Level 1

#### Description:

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config file and allow the SSH2 protocol only. This is the SSH server configuration file.

#### Rationale:

There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the

/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config file and allow the SSH2 protocol only.

**Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type Protocol and press F16 (shift F4)

Control: Protocol\_\_\_\_\_

- The display should yield the following output:

Protocol 2

**Remediation:**

EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file and explicitly define the SSH2 protocol:

- Replace:

#Protocol 2,1

- With:

Protocol 2

Re-cycle the sshd daemon to pick up the configuration changes:

#### 4.4.2 (L1) Configuring SSH – banner configuration (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config file and configure a path to a login herald message.

##### **Rationale:**

The login herald configured previously is not displayed during the initiation of a new SSH connection. Prior to a password being entered the user should accept the terms and conditions of the corporate acceptable usage policy.

##### **Audit:**

DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'

On the Control field, type Banner and press F16 (shift F4)

Control: Banner\_\_\_\_\_

The display should yield the following output:

Banner /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh\_banner

##### **Remediation:**

- Create an SSH banner file:
- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh\_banner'
- Enter appropriate text and save the file.
- NOTE: The content of the banner file can reflect any internal acceptable usage policy standards
- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file and customize the Banner parameter
- Replace:  
#Banner /some/path
- With:  
Banner /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh\_banner
- Re-cycle the sshd daemon to pick up the configuration changes:



### 4.4.3 (L1) Configuring SSH – disallow host based authentication (Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config file to ensure that host-based authentication is disallowed.

#### **Rationale:**

Using host-based authentication, any user on a trusted host can log into another host on which this feature is enabled. Since this feature depends only on system authentication and not on user authentication, it must be disabled.

#### **Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type HostbasedAuthentication and press F16 (shift F4)
- Control: HostbasedAuthentication\_\_\_\_\_
- The display should yield the following output:  
HostbasedAuthentication no

#### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file to ensure that host based authentication is disallowed:
- Replace:  
#HostbasedAuthentication no
- With:  
HostbasedAuthentication no
- Re-cycle the sshd daemon to pick up the configuration changes:

#### 4.4.4 (L1) Configuring SSH – set privilege separation (Not Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config file to ensure that privilege separation is enabled. Note, that as of OpenSSH 7.5 this configuration directive has been deprecated.

##### **Rationale:**

Setting privilege separation helps to secure remote ssh access. Once a user is authenticated the sshd daemon creates a child process which has the privileges of the authenticated user and this then handles incoming network traffic. The aim of this is to prevent privilege escalation through the initial root process.

##### **Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type UsePrivilegeSeparation and press F16 (shift F4)
- Control: UsePrivilegeSeparation \_\_\_\_\_

The display should yield the following output:

UsePrivilegeSeparation yes

##### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file to ensure that privilege separation is enabled:

- Replace:

UsePrivilegeSeparation no

- With:

UsePrivilegeSeparation yes

- Re-cycle the sshd daemon to pick up the configuration changes:

Note: In IBM i OpenSSH 6.9p1, UsePrivilegeSeparation is explicitly set to "no". Once upgrading to 8.0p1, UsePrivilegeSeparation is deprecated. There is a warning message generated when the sshd server is started when the option exists in sshd\_config. To disable the warning, you can comment out or remove the line containing UsePrivilegeSeparation from the sshd\_config file.

#### 4.4.5 (L1) Configuring SSH – set MaxAuthTries to 4 or Less (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.

##### **Rationale:**

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, it is set the number based on site policy.

##### **Audit:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type MaxAuthTries and press F16 (shift F4)
- Control: MaxAuthTries\_\_\_\_\_
- The display should yield the following output:  
MaxAuthTries 4

##### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file:
- Replace:  
#MaxAuthTries 4
- With:  
MaxAuthTries 4
- Re-cycle the sshd daemon to pick up the configuration changes:

#### 4.4.6 (L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions. When the `ClientAliveInterval` variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, sshd will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client ssh session will be terminated after 45 seconds of idle time.

##### **Rationale:**

Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

##### **Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type `ClientAliveCountMax` and press F16 (shift F4)
- Control: `ClientAliveCountMax`\_\_\_\_\_
- Verify the `ClientAliveInterval` is between 1 and 300 and `ClientAliveCountMax` is 0:  
`ClientAliveCountMax 0`  
`ClientAliveInterval 300`

##### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config' file:
- Replace:

#ClientAliveCountMax 0

#ClientAliveInterval 300

- With:

ClientAliveCountMax 0

ClientAliveInterval 300

- Re-cycle the sshd daemon to pick up the configuration changes:

#### 4.4.7 (L1) Configuring SSH – restrict Cipher list (Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

This variable limits the types of ciphers that SSH can use during communication.

##### **Rationale:**

Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBC) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

##### **Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type Ciphers and press F16 (shift F4)
- Control: Ciphers\_\_\_\_\_
- The display should yield the following output:  
Ciphers aes256-ctr,aes192-ctr,aes128-ctr

##### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd'\_config file:
- Insert:  
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
- Re-cycle the sshd daemon to pick up the configuration changes:

#### *4.4.8 (L1) Configuring SSH – Limit Access Via SSH (Not Scored)*

##### **Profile Applicability:**

- Level 1

##### **Description:**

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least of the following options be leveraged:

##### **AllowUsers**

The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

##### **AllowGroups**

The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

##### **DenyUsers**

The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

##### **DenyGroups**

The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

##### **Rationale:**

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

##### **Audit:**

- DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd\_config'
- On the Control field, type Allow and press F16 (shift F4)
- Control: Allow\_\_\_\_\_
- The display should yield the following output:

AllowUsers <userlist>

AllowGroups <grouplist>

DenyUsers <userlist>

DenyGroups <grouplist>

### **Remediation:**

- EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd'\_config file:
- Set one of the following:  
AllowUsers <userlist>  
AllowGroups <grouplist>  
DenyUsers <userlist>  
DenyGroups <grouplist>
- Re-cycle the sshd daemon to pick up the configuration changes:



## 4.5 IBM i Patch Management

### 4.5.1 (L1) IBM i Patch Management (Scored)

#### Profile Applicability:

- Level 1

#### Description:

This settings describes the IBM i patch management process.

#### Rationale:

Important IBM i updates are obtained through PTF (Program Temporary Fix) levels. Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

#### Audit:

- On a command line, type STRSQL and press Enter
- Enter the following SQL statement and press Enter.

```
SELECT ALL
```

```
GRP_CRNCY, GRP_ID, GRP_LVL, GRP_IBMLVL,  
GRP_LSTUPD, GRP_RLS, GRP_SYSSTS, GRP_TITLE  
FROM SYSTOOLS/GRPPTFCUR T01
```

```
WHERE GRP_ID IN ('SF99718', 'SF99716', 'SF99713', 'SF99223', 'SF99719')
```

- The following 5 PTF Groups should show that the INSTALLED LEVEL IS CURRENT.

```
SF99718 720 Group Security
```

```
SF99716 720 Java
```

```
SF99713 720 IBM HTTP Server for i
```

```
SF99223 720 IBM Open Source Solutions for I
```

```
SF99719 720 Group Hiper
```

#### Remediation:

Download and apply the current PTF group levels.

#### Impact:

None, this is the required process.

#### References:

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzajq/rzajqvie\\_wgrpptfcurr.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzajq/rzajqvie_wgrpptfcurr.htm)

## 4.6 System Service Tools

Service tools provide various functions that you can perform through dedicated service tools (DST) or system service tools (SST), including diagnosing system problems, managing disk units, and managing system security. With the service tools server, you can also use your PC to perform service functions through TCP/IP.

To access these service tools functions through DST, SST, IBM Navigator for i (for disk unit management), and Operations Console, service tools user IDs are required. To change or reset the passwords for the service tools user IDs, you must comply with certain password policies.

Auditors will need a System Service Tool ID with security officer privileges to audit System Service Tools. Although profiles such as QSECOFR exist in System Service Tools, they are for the most part not linked to the Operating System equivalent of QSECOFR and will most likely not have the same password.

### 4.6.1 (L1) System Service Tools Password Expiration Interval (Not Scored)

#### **Profile Applicability:**

- Level 1

#### **Description:**

This setting describes changing the System Service Tools Password Expiration Interval from the default setting, 180 days.

#### **Rationale:**

Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

The recommended state for this setting is 90 or fewer days but not 0.

#### **Audit:**

1. Access service tools using SST. On a command line, type STRSST and press Enter.
2. Select option 8 (Work with service tools user IDs and Devices)
3. Select option 6 (Work with service tools security options)
4. The value for the Password expiration interval in days should be 90.

**Remediation:**

To change the default password expiration interval from 180 days, follow these steps.

1. Access service tools using SST. On a command line, type STRSST and press Enter.
2. Select option 8 (Work with service tools user IDs and Devices)
3. Select option 6 (Work with service tools security options)
4. Change the value for the Password expiration interval in days to 90.
5. Press Enter to save changes.
6. Press F3 3 times and press Enter to exit System Service Tools.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamhchgpwdexpintval.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamhchgpwdexpintval.htm)

## *4.6.2 (L1) System Service Tools Changing the maximum failed sign-on attempts (Not Scored)*

### **Profile Applicability:**

- Level 1

### **Description:**

This policy setting determines the number of failed logon attempts before the account is locked.

The recommended state for this setting is: 3

### **Rationale:**

Setting an account lockout threshold reduces the likelihood that an attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

### **Audit:**

1. Access service tools using SST. On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 8 (Work with service tools user IDs and Devices)
4. Select option 6 (Work with service tools security options)
5. The value for the Maximum sign-on attempts allowed should be 3.

### **Remediation:**

To change the default maximum failed sign-on attempts before the user ID is disabled, follow these steps.

1. Access service tools using SST. On a command line, type STRSST and press Enter.
2. Select option 8 (Work with service tools user IDs and Devices)
3. Select option 6 (Work with service tools security options)
4. Change the value for the Maximum sign-on attempts allowed to 3.
5. Press Enter to save changes.
6. Press F3 3 times and press Enter to exit System Service Tools.

### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamhchgmaxfailedattempts.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamhchgmaxfailedattempts.htm)

### *4.6.3 (L1) System Service Tools Changing the duplicate password control (Not Scored)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

This policy setting determines the duplicate password control.

The recommended state for this setting is: 18

#### **Rationale:**

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

#### **Audit:**

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 8 (Work with service tools user IDs and Devices)
4. Select option 6 (Work with service tools security options)
5. The value for the Duplicate password control should be 18.

#### **Remediation:**

To change the default duplicate password control, complete these steps.

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Select option 8 (Work with service tools user IDs and Devices)
3. Select option 6 (Work with service tools security options)
4. Change the value for the Duplicate password control to 18.
5. Press Enter to save changes.
6. Press F3 3 times and press Enter to exit System Service Tools.

#### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamhchgduplicpwdctrl.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamhchgduplicpwdctrl.htm)



#### 4.6.4 (L1) System Service Tools Password Level (Not Scored)

##### **Profile Applicability:**

- Level 1

##### **Description:**

This policy setting determines the password level for System Service Tools.

The recommended state for this setting is: PWLVL 2

##### **Rationale:**

The default password level (PWLVL 1) uses deprecated DES encryption. To change to use SHA encryption, the System Service Tools Password Level should be set to PWLVL 2 for better security.

##### **Audit:**

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 8 (Work with service tools user IDs and Devices)
4. The value for the service tools password level should be PDLWL 2.

##### **Remediation:**

To change the default duplicate password control, complete these steps.

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Select option 8 (Work with service tools user IDs and Devices)
3. Select option 5 (Change service tools password level)
4. Press Enter to confirm your choice to set password level 2.
5. Press Enter to save changes.
6. Press F3 2 times and press Enter to exit System Service Tools.

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamh\\_pwpolicies.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamh_pwpolicies.htm)

## 4.6.5 (L1) System Service Tools Allow New Digital Certificates (Scored)

### Profile Applicability:

- Level 1

### Description:

This policy setting determines if new digital certificates can be added and also allows passwords for digital certificate stores to be reset by any user.

The recommended state for this setting is: 2

### Rationale:

Under normal operations, new digital certificates should rarely be added. More importantly, passwords for digital certificate stores should be secured from being reset by any user.

### Audit:

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 7 (Work with system security).
4. The value for the Allow new digital certificates should be 2.

### Remediation:

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 7 (Work with system security).
4. Change the value for Allow new digital certificates to 2.
5. Press Enter to save changes.
6. Press F3 3 times and press Enter to exit System Service Tools.

#### 4.6.6 (L1) System Service Tools IDs and Privileges (Not Scored)

**Profile Applicability:**

- Level 1

**Description:**

This policy setting determines the functional privileges of System Service Tool Users.

**Rationale:**

All System Service Tools Users are powerful administrators. Service Tools Users should follow the same policy as Operating System Users.

- Each Service Tool User should be unique (no shared passwords)
- Each Service Tool User should follow the Principle of Least Privilege to perform their job role
- Inactive Service Tool Users should be disabled/removed.
- IBM provides the following service tools User IDs:
  - o QSECOFR
  - o QSRV
  - o 22222222
  - o 11111111

**Audit:**

1. Type DSPSSTUSR OUTPUT(\*PRINT) and press Enter.
2. Type WRKSLPF and press Enter.
3. Locate and display your spool file named QPSYSSTUSR with User Data DSPSSTUSR.
4. Review this information with your system administrator and ensure that all SST users have unique profiles. Do not use the shipped IBM User IDs.
5. Ensure that all Service Tools IDs have the proper functional privileges for their job roles.

**Remediation:**

Disable/Remove inactive IDs and ensure that each ID has the required privileges.

**References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamh\\_recommendations.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamh_recommendations.htm)
2. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzamh/rzamh\\_srvtoolidchgprivsst.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzamh/rzamh_srvtoolidchgprivsst.htm)

#### *4.6.7 (L1) System Service Tools locking security-related system values (Scored)*

##### **Profile Applicability:**

- Level 1

##### **Description:**

This policy setting determines if users are prevented from changing security-related system values during normal operations.

The recommended state for this setting is: 2

##### **Rationale:**

During normal operations, changes to the security related system values should be locked to prevent them from being changed. Changes to security related system values should only be performed during maintenance, licensed program installations or system upgrades.

##### **Audit:**

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 7 (Work with system security).
4. The value for the Allow system value security changes should be 2.

##### **Remediation:**

1. [Access service tools using SST](#). On a command line, type STRSST and press Enter.
2. Enter a security officer service tools user ID and password on the DST Sign-On display.
3. Select option 7 (Work with system security).
4. Change the value for Allow system value security changes to 2.
5. Press Enter to save changes.
6. Press F3 3 times and press Enter to exit System Service Tools.

##### **References:**

1. [https://www.ibm.com/support/knowledgecenter/en/ssw\\_ibm\\_i\\_72/rzakz/rzakzlockunlock.htm](https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_72/rzakz/rzakzlockunlock.htm)

## 5 QSECOFR Profile

QSECOFR shall be configured with a non-trivial password which shall be transferred by the IBM i Security Officer to a document placed inside a sealed envelope and stored in a secure location such as a bank vault or secure on-site lock box or safe. QSECOFR's password shall not be shared or used under normal system operations and shall only be used in emergencies.

The password shall be changed at regular intervals and replaced in the secure location.

### 5.1 (L1) QSECOFR Profile Shall Be \*DISABLED (Scored)

#### Profile Applicability:

- Level 1

#### Description:

The QSECOFR profile shall be \*DISABLED to prevent interactive use. You can always sign on with the QSECOFR profile at the console, even if the status of QSECOFR is \*DISABLED.

#### Rationale:

QSECOFR is the most powerful profile on the IBM i and is equivalent to the UNIX Root Profile. Additionally, you should prevent QSECOFR from interactively signing on by \*DISABLING it and create unique security officer profiles as required by the business.

#### Audit:

- DSPUSRPRF USRPRF(QSECOFR)
- Observe the Status to ensure that it is \*DISABLED

#### Remediation:

CHGUSRPRF USRPRF(QSECOFR) STATUS(\*DISABLED)

#### Impact:

\*DISABLEing QSECOFR will prevent anonymous and un-accountable use of QSECOFR for normal operations.

## 5.2 (L1) QSECOFR Shall Not be Configured as a Group Profile (Scored)

### Profile Applicability:

- Level 1

### Description:

QSECOFR shall not be a group profile as this would allow group members to inherit root privileges from the shipped IBM QSECOFR profile.

### Rationale:

Do not use IBM profiles as groups. Instead, create your own group profiles with appropriate privileges (special authorities) commensurate with your job roles and the Principle of Least Privilege (PoLP).

### Audit:

DSPUSRPRF USRPRF(QSECOFR) TYPE(\*GRPMBR)

Ensure that message states that "User profile QSECOFR not a group profile".

### Remediation:

Change any QSECOFR group members to another user created group with appropriate privileges (special authorities) commensurate with your job roles and the Principle of Least Privilege (PoLP).

- CHGUSRPRF USRPRF(<XXXXXX>) GRPPRF(<XXXXXX>)

## 6 Auditing

Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged administrative methods. The IBM i security audit journal, associated journal receivers and receiver library shall be secured as follows:

- QAUDJRN = \*PUBLIC \*EXCLUDE and owned by QSYS
- Associated QAUDJRN journal receivers = \*PUBLIC \*EXCLUDE and owned by QSYS
- Associated QAUDJRN library = \*PUBLIC \*EXCLUDE and owned by QSYS

Relevant security events shall be examined on a regular basis to determine if attacks or malicious activity has occurred. Audit logs must be retained according to policy and/or regulatory requirements.

## **7 Monitoring**

The IBM i must be monitored to ensure compliance network security policies and standards. Security personnel must test the IBM i configuration and security controls for effectiveness and compliance.

## **8 Documentation**

Procedures to implement IBM i security must be documented. User accounts and associated privileges must be documented. All documentation must be reviewed at least annually to ensure compliance with network security policies and standards. Account documentation must be reviewed quarterly to ensure that it is current and accurate. Documentation must be stored in a secure location and must be readily available.

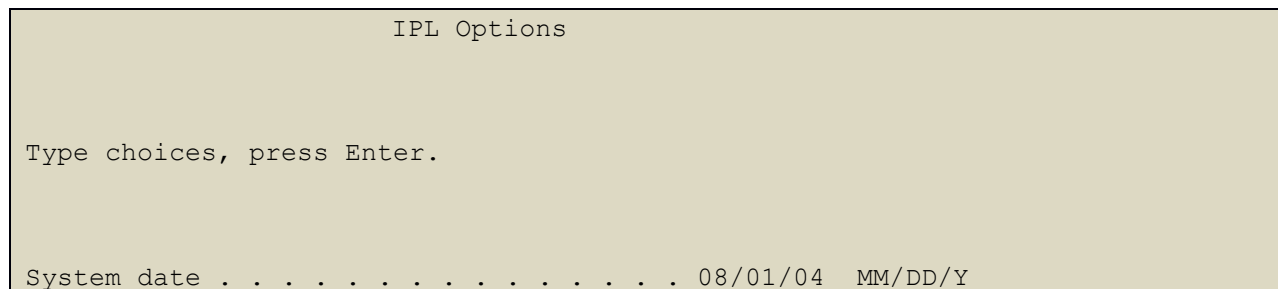
## **9 Physical Security**

There must be strong physical security around the IBM i server. All production IBM i servers need to be housed in physically secure environments with limited access.

## **10 Disaster Recovery**

During a complete disaster recovery after a catastrophic system failure, some of the system values in Table 1 will need to be changed to allow a full system restore. Follow the normal procedures found in IBM i Backup & Recovery (SC41-5304) and then follow the steps below:

- After the LIC and Operating System restore completes, you will see the IPL Options screen. On the IPL Options screen, ensure that the “Define or change system at IPL” option is set to Y for yes as shown below.



```
IPL Options

Type choices, press Enter.

System date . . . . . 08/01/04  MM/DD/Y
```



|  |          |             |
|--|----------|-------------|
| System time . . . . .                      | 16:58:00 | HH:MM:S     |
| System time zone . . . . .                 | Q0000UTC | F4 for list |
| Clear job queues . . . . .                 | N        | Y=Yes, N=NO |
| Clear output queues . . . . .              | N        | Y=Yes, N=NO |
| Clear incomplete job logs . . . . .        | N        | Y=Yes, N=NO |
| Start print writers . . . . .              | N        | Y=Yes, N=NO |
| Start system to restricted state . . . . . | Y        | Y=Yes, N=NO |
| Set major system options . . . . .         | Y        | Y=Yes, N=NO |
| Define or change system at IPL . . . . .   | Y        | Y=Yes, N=NO |

- On the Set Major System Options screen, select Y to enable automatic configuration.
- Select 3, System Value Commands.
- On the System Value Commands screen, select 3, Work with System Values.
- On the Work with System Values screen, select the System Value that you plan to change by placing a "2" next to it. Press Enter ONLY after you select all the values that you wish to change.
- Update the following System Values. Write down the existing values so you can update them after the recovery, if necessary.
  - Change QALWOBJRST to \*ALL
  - Change QJOBMSGQFL to \*PRTWRAP
  - Change QJOBMSGQMX size to a minimum value of 30
  - Change QPFRADJ to 2
  - Change QVIFYOBJRST to 1
  - Change QFRCCVNRST to 0

After changing the system values listed above and restoring your licensed programs and user data, set the system values back to the previous value that you wrote down above and ensure that they meet the standards value in Table 1.

## 11 Licensed Program Installation Procedure

During an installation of IBM i licensed program options and products, the following system values require a change. Write down the current value prior to changing and change it back to its previous value when the licensed program installation is complete.

- Change QALWOBJRST to \*ALL

# Appendix: Summary Table

| Control      |  | Set Correctly            |                          |
|--------------|--|--------------------------|--------------------------|
|              |  | Yes                      | No                       |
| <b>1</b>     | <b>Access Control</b>  |                          |                          |
| <b>2</b>     | <b>Adopted Authority</b>   |                          |                          |
| <b>3</b>     | <b>User Profiles</b>   |                          |                          |
| 3.1          | (L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority) (Scored) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2          | (L1) User Profile (*USRPRF) Access Controls (Private authority) (Scored) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3          | (L1) User Profile (*USRPRF) Object Ownership (Scored)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4          | (L1) Administrative Special Authorities (Not Scored)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5          | (L1) User Profile Action Auditing (Scored)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6          | (L1) Default Passwords (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7          | (L1) Inactive Profiles (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.8          | (L1) User Profile With Non-Expiring Passwords (Not Scored)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.9          | (L1) User Profiles With Command Line Access (Not Scored)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.10         | (L1) IBM Supplied User Profiles (Not Scored)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.11         | (L1) Group Profiles With Passwords (Scored)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4</b>     | <b>System Configuration</b>  |                          |                          |
| <b>4.1</b>   | <b>Security System Values</b>  |                          |                          |
| <b>4.1.1</b> | <b>Level 1</b>   |                          |                          |
| 4.1.1.1      | (L1) Allow Restoration of Security-Sensitive Objects (Scored)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2      | (L1) Set Attention Program (Scored)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3      | (L1) Set Auditing Control (Scored)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4      | (L1) Set Auditing End Action (Scored)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5      | (L1) Set Auditing Force Level (Scored)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.6      | (L1) Set Auditing Level (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.7      | (L1) Set Security Auditing Level Extensions (Scored)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.8      | (L1) Set Automatic Device Configuration (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.9      | (L1) Set Automatic Remote Controller Configuration (Scored)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.10     | (L1) Set Automatic Virtual Device Creation (Scored)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.11     | (L1) Set Create Authority (Scored)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.12     | (L1) Set Disconnect-Job Interval (Scored)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.13     | (L1) Set Display User Sign-on Information (Scored)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.14     | (L1) Set Force Conversion On Restore (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.15     | (L1) Set Inactivity Time-out Interval (Scored)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.16     | (L1) Set Inactivity Message Queue (Scored)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.17     | (L1) Set Limit Device Sessions (Scored)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.18     | (L1) Set Limit Security Officer Access to Workstations                   | <input type="checkbox"/> | <input type="checkbox"/> |

|              |  |                          |                          |
|--------------|--|--------------------------|--------------------------|
|              | (Scored)   |                          |                          |
| 4.1.1.19     | (L1) Set Maximum Sign-on Action (Scored)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.20     | (L1) Set Maximum Sign-on Attempts (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.21     | (L1) Set Block Password Change (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.22     | (L1) Set Password Expiration Interval (Scored)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.23     | (L1) Set Password Expiration Warning (Scored)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.24     | (L1) Set Password Level (Scored)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.25     | (L1) Set Required Difference in Passwords (Scored)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.26     | (L1) Set Password Rules (Scored)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.27     | (L1) Retain Server Security (Scored)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.28     | (L1) Set Remote IPL (Scored)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.29     | (L1) Set Remote Sign-on Value (Scored)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.30     | (L1) Set Remote Service Attribute (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.31     | (L1) Scan File System (Scored)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.32     | (L1) Set Scan File System Control (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.33     | (L1) Set System Security Level (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.34     | (L1) Set Shared Memory Control (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.35     | (L1) Secure Sockets Layer (SSL) cipher specification list (Scored) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.36     | (L1) Set Transport Layer Security cipher control (Scored)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.37     | (L1) Transport Layer Security protocols (Scored)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.38     | (L1) System Library List (Scored)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.39     | (L1) Set Use Adopted Authority (Scored) (Scored)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.40     | (L1) Verify Object On Restore (Scored) (Scored)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.1.2</b> | <b>Level 2</b>   |                          |                          |
| 4.1.2.1      | (L2) Allow Restoration of Security-Sensitive Objects (Scored)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.2      | (L2) Allow User Domain Objects in These Libraries (Scored)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.3      | (L2) Set Auditing Control (Scored)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.4      | (L2) Set Auditing End Action (Scored)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.5      | (L2) Set Auditing Force Level (Scored)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.6      | (L2) Set Automatic Virtual Device Creation (Scored)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.7      | (L2) Set Create Authority (Scored)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.8      | (L2) Set Create Object Audit Level (Scored)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.9      | (L2) Set Disconnect-Job Interval (Scored)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.10     | (L2) Set Force Conversion On Restore (Scored)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.11     | (L2) Set Inactivity Time-out Interval (Scored)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.12     | (L2) Set Inactivity Message Queue (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.13     | (L2) Set Limit Device Sessions (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.14     | (L2) Set Limit Security Officer Access to Workstations (Scored)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.15     | (L2) Set Maximum Sign-on Action (Scored)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.16     | (L2) Set Maximum Sign-on Attempts (Scored)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.17     | (L2) Set Block Password Change (Scored)                            | <input type="checkbox"/> | <input type="checkbox"/> |

|            |   |                          |                          |
|------------|---|--------------------------|--------------------------|
| 4.1.2.18   | (L2) Set Password Level (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.19   | (L2) Set Required Difference in Passwords (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.20   | (L2) Set Password Rules (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.21   | (L2) Set Password Validation Program (Scored) (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.22   | (L2) Set Remote Sign-on Value (Scored) (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.23   | (L2) Retain Server Security (Scored) (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.24   | (L2) Set System Security Level (Scored) (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.25   | (L2) Set Shared Memory Control (Scored) (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2.26   | (L2) Verify Object On Restore (Scored) (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.2</b> | <b>Network Services</b>   |                          |                          |
| 4.2.1      | (L1) Network Attribute JOBACN (Network Job Action) (Scored)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.2      | (L1) DDM Remote Configuration List (SNA) Attributes (Scored)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.3      | (L1) DDM TCP/IP Attributes (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.4      | (L1) Telnet Protocol (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2.5      | (L1) FTP Protocol (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.3</b> | <b>IBM i Netserver security</b>   |                          |                          |
| 4.3.1      | (L1) IBM i NetServer Guest Profile (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.2      | (L1) IBM i NetServer LANMAN Password Hash (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.3      | (L1) IBM i SMB Signing (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.4      | (L1) IBM i SMBv2 Server (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.5      | (L1) IBM i NetServer Shares (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3.6      | (L2) NetServer Browse Interval (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.4</b> | <b>IBM i SSH Server security</b>  |                          |                          |
| 4.4.1      | (L1) Configuring SSH – server protocol 2 (Scored)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.2      | (L1) Configuring SSH – banner configuration (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.3      | (L1) Configuring SSH – disallow host based authentication (Scored)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.4      | (L1) Configuring SSH – set privilege separation (Not Scored)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.5      | (L1) Configuring SSH – set MaxAuthTries to 4 or Less (Scored)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.6      | (L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Scored) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.7      | (L1) Configuring SSH – restrict Cipher list (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4.8      | (L1) Configuring SSH – Limit Access Via SSH (Not Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.5</b> | <b>IBM i Patch Management</b>   |                          |                          |
| 4.5.1      | (L1) IBM i Patch Management (Scored)  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4.6</b> | <b>System Service Tools</b>   |                          |                          |
| 4.6.1      | (L1) System Service Tools Password Expiration Interval (Not Scored)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6.2      | (L1) System Service Tools Changing the maximum failed sign-on attempts (Not Scored)             | <input type="checkbox"/> | <input type="checkbox"/> |

|           |  |                          |                          |
|-----------|--|--------------------------|--------------------------|
| 4.6.3     | (L1) System Service Tools Changing the duplicate password control (Not Scored) | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6.4     | (L1) System Service Tools Password Level (Not Scored)                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6.5     | (L1) System Service Tools Allow New Digital Certificates (Scored)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6.6     | (L1) System Service Tools IDs and Privileges (Not Scored)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6.7     | (L1) System Service Tools locking security-related system values (Scored)      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5</b>  | <b>QSECOFR Profile</b>   |                          |                          |
| 5.1       | (L1) QSECOFR Profile Shall Be *DISABLED (Scored)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2       | (L1) QSECOFR Shall Not be Configured as a Group Profile (Scored)               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6</b>  | <b>Auditing</b>  |                          |                          |
| <b>7</b>  | <b>Monitoring</b>  |                          |                          |
| <b>8</b>  | <b>Documentation</b>   |                          |                          |
| <b>9</b>  | <b>Physical Security</b>   |                          |                          |
| <b>10</b> | <b>Disaster Recovery</b>   |                          |                          |
| <b>11</b> | <b>Licensed Program Installation Procedure</b>                                 |                          |                          |

# Appendix: Change History

| Date | Version | Changes for this version |
|------|---------|--------------------------|
|      |         |                          |