# Assure Security Risk Assessment

| | |
|---|---|
| **Name:** | **S21D162V** |
| **Serial #:** | **21D162V** |
| **Model:** | **E4D** |
| **OS Version:** | **V7R2M0** |
| **Date:** | **2019-07-19** |
| **Assessment type:** | **FULL** |

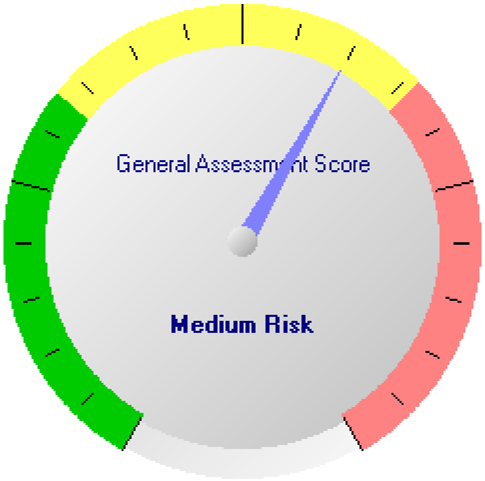
## PLEASE NOTE

This report is not an audit. You should not regard it as a mini-audit nor as a security policy or the implementation of such a policy. The aim of this report is to make you aware of security exposure in policy or implementation as well as to make you aware of missing parts in a policy or implementation or of areas where security policy may deviate from system configuration.

It is recommended to test any recommendations in this report in an environment that is similar to your production environment. The recommendations in this report are based on the Syncsort understanding with IBM i security options and documentation; however it is impossible to predict whether these recommendation will affect your environment as well as with your specific applications.

## Table of Contents

# Management Summary



**This security assessment examines a selection of security definitions on your system. These are split into 4 main categories as follows:**

**1. System Values**
**2. User Profiles**
**3. Object Authorities**
**4. Access through Network**

**The details and findings of each check are listed in the subsequent pages. They are compared with generally accepted industry best practices.**

**In all, a total of 57 checks were made across all categories, of these 10 followed recommended best practice, 25 should be reviewed and 22 constitute a significant security risk.**

**Your policies for Access through Network have vulnerabilities that should be reviewed and corrected where possible.**

**For System Values definitions, your policy exposes your system to high risk and this should be addressed urgently; other weak definitions should be reviewed and corrected where possible.**

**Regarding user profiles, these too expose your system to high risk and this should be addressed as soon as possible; additional weak definitions should be reviewed and corrected where possible.**

**In addition, the object authorities in your system are found to be at risk and should be addressed as soon as possible.**

**Finally, a list of ports in listening mode are included. Open ports cannot be completely avoided but they should be closely monitored and those that are not expected to be used should be prevented from being opened.**

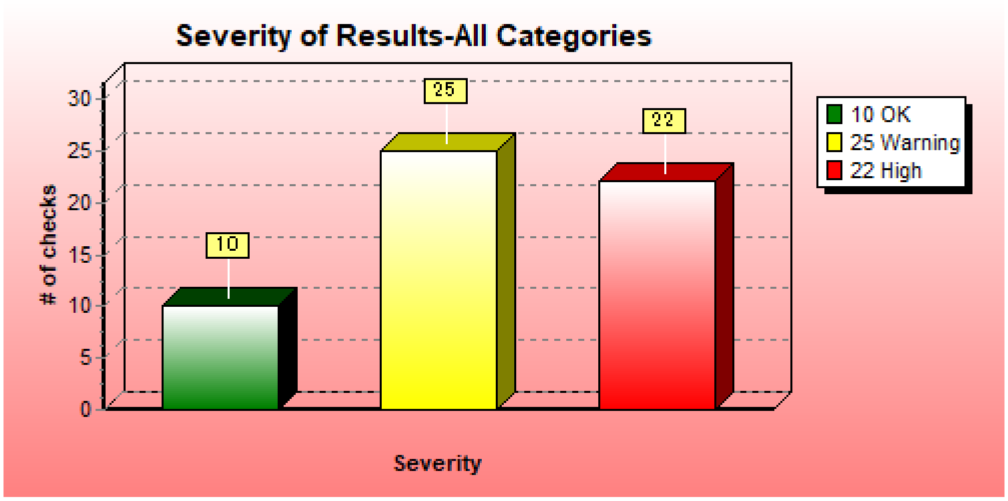
**The conclusions are divided to three different severities:**

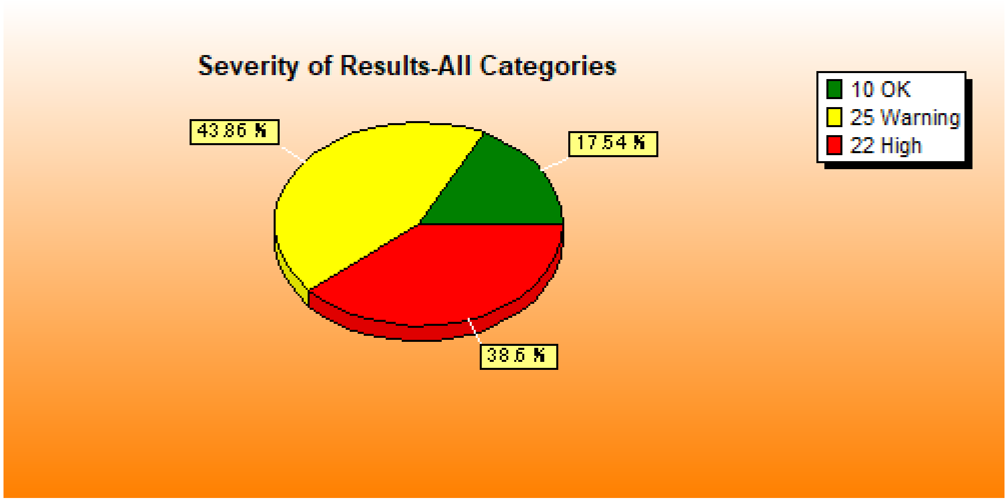
| | |
|---|---|
| ✓ Severity - OK | Following recommended best practice |
| ⚠ Severity - Warning | Some risk present |

| | |
|---|---|
| R Severity - High | Significant security risk present |

**Summary of Severities for each Category:**

| Category | # of checks | OK | Warning | High Risk |
|---|---|---|---|---|
| System Values | 23 | 6 | 11 | 6 |
| User Profiles | 19 | 3 | 6 | 10 |
| Object Authorities | 13 | 1 | 6 | 6 |
| Access through Network | 2 | 0 | 2 | 0 |
| Total | 57 | 10 | 25 | 22 |





# Assessment Details

## System Values

### System Value: QALWOBJRST - Allow object restore option

**Current Value: *ALL**

Specifies whether or not objects with security-sensitive attributes can be restored. This value is made up of a list of values that control the object being restored. The value can be specified as *ALL, *NONE, or a list of values. If *ALL or *NONE is specified, no other values are allowed. A change to this system value takes effect at the start of the next restore operation.

When an attempt is made to restore an object onto the system, three system values work together as filters to determine if the object is allowed to be restored, or if it is converted during the restore. The first filter is the verify object on restore QVFYOBJRST system value. It is used to control the restore of some objects that can be digitally signed. The second filter is the force conversion on restore   QFRCCVNRST system value. This system value allows you to specify whether or not to convert programs, service programs, SQL packages, and module objects during the restore. It can also prevent some objects from being restored. Only objects that can get past the first two filters are processed by the third filter. The third filter is the allow object on restore (QALWOBJRST) system value. It specifies whether or not objects with security-sensitive attributes can be restored.

**Analysis and Recommendations:**

R Set to *ALWPTF. The current setting allows any object to be restored by a user with the correct authority. A recommended setting for this value is *ALWPTF or *NONE. *ALWPTF will allow system-state or inherit-state programs, service programs, modules, objects that adopt authority, objects that have the S_ISUID (set-user-ID) attribute enabled, and objects that have the S_ISGID (set-group-ID) attribute enabled to be restored to the system during a PTF install. *NONE does not allow objects with security-sensitive attributes to be restored.

### System Value: QAUDCTL - Auditing control

**Current Values:**

*AUDLVL
*OBJAUD
*NOQTEMP

The audit control (QAUDCTL) system value contains the values to turn on object and user action auditing to the System Journal. It also includes value for skipping QTEMP objects.

**Analysis and Recommendations:**

✓ The value is set according to recommended best practice. The recommended settings for this system value are: *NOQTEMP, *OBJAUD, and *AUDLVL.

## System Value: QAUDLVL - Security auditing level

**Current Values:**

*AUDLVL2

The security auditing level (QAUDLVL) system value controls the level of action auditing on the system.

**Analysis and Recommendations:**

⚠ The current value does not have all of the recommended values which can limit and/or exclude the recommended auditing capabilities of the QAUDJRN. The recommended settings for this system value are: *AUTFAIL, *CREATE, *DELETE, *JOBDTA, *OBJMGT, *PGMFAIL, *SAVRST, *SECURITY, *SERVICE, and *SYSMGT.

## System Value: QCRTAUT - Create default public authority

**Current Value: *CHANGE**

Create authority. Specifies the default public authority used when objects are created into a library. When the *LIBCRTAUT value of the AUT keyword of a create object command is used to set public authority for an object, the CRTAUT value of the library where the object is being created determines what public authority will be used for the object. If the CRTAUT value of the library is set to *SYSVAL, the value specified in the QCRTAUT system value is used to set the public authority for the object being created.

Changing the QCRTAUT system value to a more restrictive value of *USE or *EXCLUDE limits access of newly created objects. The owner of the objects, or the security officer, may need to grant additional authority before the object can be used. An example of this is signing on a newly created device. When the device is created by either the CRTDEVDSP command or automatic configuration, the public authority is set to *USE or *EXCLUDE. Because *CHANGE authority to the device description is required in order to sign on the system, the sign-on will not be allowed.

**Analysis and Recommendations:**

R Set to *EXCLUDE. The recommended setting for this value is *EXCLUDE which will set the default public authority for newly created objects to *EXCLUDE.

## System Value: QFRCCVNRST - Force conversion on restore

**Current Value: 0**

The Force Conversion on Restore (QFRCCVNRST) system value can force the conversion of some object types during a restore. This system value can also prevent some objects from being restored. QFRCCVNRST is the second of three system values that work consecutively as filters to determine if an object is allowed to be restored, or if it is converted during the restore. The first filter, Verify Object on Restore (QVFYOBJRST) system value, controls the restore of some objects that can be digitally signed. Only objects that can get past the first two filters are processed by the third filter, the Allow Object Restore (QALWOBJRST) system value, which specifies whether objects with security-sensitive attributes can be restored. The shipped value of QFRCCVNRST is 1.

**Analysis and Recommendations:**

⚠ With this system setting, objects from older operating system formats might be restored without conversion or get converted even if they have validation errors. The recommended setting for this value is 3 or higher. 3 = Objects which are suspected of having been tampered with, objects which contain validation errors, and objects which require conversion to be used on the current version of the operating system or on the current machine will be converted.

4 = Objects which contain sufficient creation data to be converted and do not have valid digital signatures will be converted. An object that does not contain sufficient creation data will be restored without conversion.

Note: Objects (signed and unsigned) that have validation errors, are suspected of having been tampered with, or require conversion to be used on the current version of the operating system or on the current machine will be converted; or will fail to restore if they do not convert.

5 = Objects that contain sufficient creation data will be converted. An object that does not contain sufficient creation data to be converted will be restored.

Note: Objects that have validation errors, are suspected of having been tampered with, or require conversion to be used on the current version of the operating system or on the current machine that cannot be converted will not restore.

6 = All objects which do not have a valid digital signature will be converted.

Note: An object with a valid digital signature that also has a validation error or is suspected of having been tampered with will be converted, or if it cannot be converted, it will not be restored.

7 = Every object will be converted.

## System Value: QMAXSIGN - Maximum sign-on attempts allowed

**Current Value: 3**

The maximum sign-on attempts allowed (QMAXSIGN) system value controls the number of consecutive sign-on or password verification attempts that are not correct by local and remote users. When the maximum number of sign-on or password verification attempts is reached, the (QMAXSGNACN) system value is used to determine the action to be taken.

**Analysis and Recommendations:**

✅ The value is set correctly according to current industry standards. The recommended setting for this system value is 3 - a user can try a maximum of 3 sign-on or password verification attempts.

## System Value: QPWDEXPITV - Password expiration interval

**Current Value: *NOMAX**

Specifies the number of days for which passwords are valid. This provides password security by requiring users to change their passwords after a specified number of days. If the password is not changed within the specified number of days, the user cannot sign-on until the password is changed. Seven days before the password ends, you are warned at sign-on time, even if you are not displaying sign-on information (the system value QDSPSGNINF).

The password expiration interval for your system is defined in system value QPWDEXPITV, which is currently set to *NOMAX .

**Analysis and Recommendations:**

R A password expiration interval value of *NOMAX allows users to never change their passwords. This gives hackers unlimited time to try and discover passwords. We recommend using the System Value QPWDEXPITV on your User Profiles to control their password expiration interval. This insures that passwords for User Profiles are changed on a regular basis determined centrally by your company policy. Without this, each user could have a different interval which could include longer periods of time beyond the company policy or more troubling a value of *NOMAX. A value *NOMAX means that the password does not expire which allows intruders an indefinite period of time to obtain or guess the password.

## System Value: QPWDLMTAJC - Limit Adjacent Digits in Password

**Current Value: 0**

Specifies whether adjacent numbers are allowed in passwords. This makes it difficult to guess passwords by preventing the use of dates or social security numbers as passwords. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

Limitation of sequences in passwords (also referred to as adjacent digits) for your system is defined in system value QPWDLMTAJC, which is currently set to 0 .

⚠ Set the value to 1 - adjacent numbers not allowed. This will prevent the use of sequential numbers in the password such as 123, which are commonly used by users and makes the password easier to guess and generate.

## System Value: QPWDLMTCHR - Limit Characters in Password

**Current Value: *NONE**

This provides password security by preventing certain characters (vowels, for example) from being in a password. This makes it difficult to guess passwords by preventing the use of common words or names as passwords. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

✓ This value follows recommended best practice. We therefore recommend a value of *NONE unless there are technical limitations that prevent certain characters them from being used (such limitations have been existent in older computing environments but are rarely seen today).

## System Value: QPWDLMTREP - Limit repeating characters in password

**Current Value: 0**

This prevents a user from using the same character more than once in the same password. (For example, AAAA.) A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

⚠ The current value does not prevent users from repeating characters in their passwords. If all users can be trusted to create complex passwords, then this value is acceptable. If however there is reason to suspect they might choose simple passwords with repeating characters, a better policy is needed. We therefore recommend a value of 2 (cannot be repeated consecutively). This will not prevent every simple password combination (such as a1a1a1) but blocks easily breakable passwords like jonnyb11 and additionally allows a reasonably high number of character combinations and flexibility

## System Value: QPWDLVL - Password Level

**Current Value: 0**

Specifies the level of password support on the system. The password level of the system can be set to allow for user profile passwords from 1-10 characters or to allow for user profile passwords from 1-128 characters. Changing the password level of the system from 1-10 character passwords to 1-128 character passwords requires careful consideration. If your system communicates with other systems in a network, then all systems must be able to handle the longer passwords.

**Analysis and Recommendations:**

⚠ Set value to 2 to allow passwords up to 128 characters. This keyword controls maximum password length and the use of upper and lower case. 0 and 1 support up to 10 characters that are automatically converted to uppercase and 2 and 3 support up to 128 characters in upper and lower case. 1 and 3 are similar to 0 and 2 respectively, but IBM i Netserver passwords for Windows 98/95/ME are removed from the system. 2 and 3 are more secure than 0 and 1 as they allow far more combinations and flexibility in the choice of password.
Our recommendation therefore is 3 wherever possible and 2 if you still use NetServer for old Microsoft Windows versions.

## System Value: QPWDMAXLEN - Maximum Password Length

**Current Value: 10**

Specifies the maximum number of characters in a password. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

⚠ The current value allows users to create passwords longer than IBM's recommendation, but this is still less than the maximum allowed.   We recommend removing all possible limitations on maximum password length and that means setting the value to 128.

## System Value: QPWDMINLEN - Minimum Password Length

**Current Value: 6**

Specifies the minimum number of characters in a password. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

⚠ The current value of 6 is no longer the recommended value by IBM and many others. It has been superseded with a recommendation of 7.   We therefore recommend hardening this setting to a system value of 8.

## System Value: QPWDPOSDIF - Limit Password Character Positions

**Current Value: 0**

This system value controls the position of characters in a new password. This prevents the user from specifying the same character in a password corresponding to the same position in the previous password. For example, new password DJS2 could not be used if the previous password was DJS1 (the D, J, and S are in the same positions). A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

⚠ The value is not set according to our recommendation. A better solution, not available in the IBM i at this time, would be to implement this restriction for a set number of characters e.g. to force the change of at least 3 characters. However, in the absence of such an option, we recommend a value of 1 as this addresses the bigger risks such as incrementing a single number.

## System Value: QPWDRQDDGT - Require Digit in Password

**Current Value: 0**

Specifies whether a digit is required in a new password. This prevents the user from only using alphabetic characters. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

R The current setting does not afford optimal security. Forcing a password to contain at least 1 digit prevents the use of very simple passwords such as those constructed from a single word or name. It also increases the complexity of the password and makes it more difficult to guess. Today, still more elaborate rules can be found to control password structure, such as forced inclusion of special characters. In the absence of more elaborate password rules, forced inclusion of a digit is a wise policy and so we recommend a value of 1 - required.

## System Value: QPWDRQDDIF - Duplicate Password Control

**Current Value: 0**

The number of unique passwords that are required before a password can be repeated. With a value of 1 the last 32 passwords can't be reused, value of 2 the last 24 passwords, value of 3 the last 18 passwords, value of 4 the last 12 passwords, value of 5 the last 10 passwords, value of 6 the last 8 passwords, value of 7 the last 6 passwords, and value of 8 the last 4 passwords. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

R The current setting is not secure as it allows password 'changes' to be submitted in which the new password is identical to the previous one. Allowing reuse of a password that has been used in the past is bad practice. It can lead to increased chances of penetrating the system using an old password which may have been discovered. The recommended value is therefore 1 (can't be last 32).

## System Value: QPWDRULES - Password rules

### Current Values:

*PWDSYSVAL

Specifies the rules used to check whether a password is formed correctly. Changes made to this system value take effect the next time a password is changed.

### Analysis and Recommendations:

⚠ You are not yet using the QPWDRULES system value. It is recommended to switch to using this instead of the individual system values it replaces because it gives more flexibility and control.

The QPWDRULES system value - introduced in i/OS v7.1 - is an enhancement to password control that optionally replaces 7 older system values: QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF and QPWDRQDDGT.

The default value for QPWDRULES is *PWDSYSVAL, which instructs the operating system to refer to the 7 system values above. It can be replaced with one or more of 23 different parameters defining various different rules for password format. *PWDSYSVAL cannot be combined with other parameters. Once a value other than *PWDSYSVAL is provided for QPWDRULES, all system values mentioned above are ignored.

All Parameters:

| | |
|---|---|
| *CHRLMTAJC: | Cannot contain the same character (any type - alphanumeric or special character) in any 2 consecutive positions. |
| *CHRLMTREP: | Cannot contain the same character more than once anywhere in the password. |
| *DGTLMTAJC: | Cannot contain the same digit in any 2 consecutive positions |
| *DGTLMTFST: | First position cannot be a digit. |
| *DGTLMTLST: | Last position cannot be a digit. |
| *DGTMAXn: | Maximum number of digits, where n is 0-9. |
| *DGTMINn: | Minimum number of digits, where n is 0-9. |
| *LMTSAMPOS: | Equivalent to QPWDPOSDIF. See description above |
| *LMTPRFNAME: | Cannot contain complete user name |
| *LTRLMTADJ: | Cannot contain the same alphabetic character in any 2 consecutive positions. |
| *LTRLMTFST: | First position cannot be a letter. |
| *LTRLMTLST: | Last position cannot be a letter. |
| *LTRMAXn: | Maximum number of letters, where n is 0-9. |
| *LTRMINn: | Minimum number of letters, where n is 0-9. |
| *MAXLENnnn: | Equivalent to QPWDMAXLEN. See description above |
| *MINLENnnn: | Equivalent to QPWDMINLEN. See description above |
| *MIXCASEn: | Minimum required number of n uppercase and n lower case letters, where n is 0-9. For PWDLVL 2 and 3 only. |
| *REQANY3: | Must contain characters from at least 3 of these 4 groups: uppercase, lowercase, digit or special. |
| *SPCCHRLMTADJ: | Cannot contain the same special character in any 2 consecutive positions. |
| *SPCCHRLMTFST: | First position cannot be a special character. |
| *SPCCHRLMTLST: | Last position cannot be a special character. |

*SPCCHRMAXn: Maximum number of special characters required, where n is 0-9
*SPCCHRMINn: Minimum number of special characters required, where n is 0-9.

## System Value: QPWDVLDPGM - Password Validation Program

**Current Value: *NONE**

This provides the ability for a user-written program to do additional validation on passwords. The program must exist in the system auxiliary storage pool (ASP) or in a basic user ASP. A change to this system value takes effect the next time a password is changed.

**Analysis and Recommendations:**

✓ You are not using a password validation program and this is in accordance with our recommended best practice.
The existence of a user-written program in the system that receives readable passwords constitutes a security risk that in our opinion advocates non-usage of this option. We recommend changing this value to *NONE and making use of the QPWDRULES system value instead.

## System Value: QRETSVRSEC - Retain server security data

**Current Value: 0**

Determines whether the security data needed by a server to authenticate a user on a target system through client-server interfaces can be retained on the host system. A change to this system value takes effect immediately.

**Analysis and Recommendations:**

⚠ Set to 1, because a value of 0 will cause application failure when web servers, IBM i code or applications require data that is encryptable and decryptable. QRETSVRSEC was originally implemented to provide a layer of security that is no longer necessary. The recommended setting for this value is 1 which retains decryptable authentication information associated with user profiles or validation list (*VLDL) entries. You must have *ALLOBJ and *SECADM special authorities to change the QRETSVRSEC system value.

## System Value: QSECURITY - System security level

**Current Value: 40**

Specifies the level of security on the system. A change to this system value takes effect at the next IPL.

**Analysis and Recommendations:**

✓ The value is set correctly according to current industry standards. The recommended setting for this value is 40 or 50. The system requires a password to sign on and users must have authority to access objects and system resources. With Level 40, programs fail if they try to access objects through interfaces that are not supported. With Level 50, programs fail if they try to pass unsupported parameter values to supported interfaces or if they try to access objects through interfaces that are not supported.

## System Value: QSHRMEMCTL - Shared memory control

**Current Value: 1**

Controls whether or not users are allowed to use shared memory or mapped memory that has write capability. You must have *ALLOBJ and *SECADM special authorities to change this system value.

**Analysis and Recommendations:**

✓ The value is set correctly according to current industry standards. The recommended setting for this value is 1. Users can use shared memory or mapped memory that has write capability. Use this value in environments where pointers may be shared among programs between different jobs.

## System Value: QUSEADPAUT - Use adopted authority

**Current Value: *NONE**

Defines which users can create programs with the use adopted authority (*USEADPAUT (*YES)) attribute. QUSEADPAUT defaults to *NONE. All users can create, change, or update programs and service programs to use adopted authority if the user has the necessary authority to the program or service program. This parameter can also contain the name of an authorization list. The user's authority is checked against this authorization list. If the user has at least *USE authority to the named authorization list, the user can create, change, or update programs or programs with the USEADPAUT (*YES) attribute. A change to this system value takes effect when the user's programs are created.

**Analysis and Recommendations:**

⚠ Create a validation list containing user profiles permitted to create, change or update programs to use adopted authority and then save the validation list name in this system value. The recommended setting for this value is to have an authorization list defined. This validation list is used to control who can set adopted authority.

## System Value: QVFYOBJRST - Verify object on restore

**Current Value: 1**

The Verify Object on Restore (QVFYOBJRST) system value determines whether objects are required to have digital signatures in order to be restored to your system.

**Analysis and Recommendations:**

R The current setting is lower than recommended. Unless you have good reason to restore signed objects that you expect will fail signature validation. It is recommended to change setting to 3. The recommended setting for this value is 3 to verify signatures on restore. Restore unsigned commands and user-state objects. Restore signed commands and user-state objects only if the signatures are valid.
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.

## Supplemental Report Reference: SRA001 - System Values

# User Profiles

## Profiles with Password Expiration not *SYSVAL

Passwords should be set to expire within a reasonable amount of time. This provides security to the User Profiles from hackers or internal disgruntled employees. If the Password Expiration parameter on a User Profile is set to *NOMAX or a high number of days, this makes it vulnerable to attack.

R Out of a total of 75 user profiles in your system, 5 user profiles have a password expiry interval that is not controlled centrally by the QPWDEXPITV system value. Out of these 5 user profiles, 3 are enabled and have passwords, meaning they can currently sign on to the system.

Out of 5 users that have expiry not *SYSVAL, 5 users have *NOMAX, 0 users have number of days less than system value (which is good), and 0 users have parameter more than *SYSVAL.

Most user profiles should have their password expiry interval set by system value. If you choose to allow certain user profiles ensure they are still within your desired policy.

User profiles can be reviewed and changed using the WRKUSRPRF, DSPUSRPRF and CHGUSRPRF commands. An alternative and more efficient method is to define and monitor and set your password expiration policy using the Enforcive Compliance module, user profile template

**Supplemental Report Reference: SRA002 - User Profile Information**

## Distribution of Powerful Users

R Out of 23 non-IBM users that are in the system 18 powerful users are defined. The number of powerful users is much more than what is recommended and this puts the system at risk of someone abusing one of these user profiles.

### By Special Authority

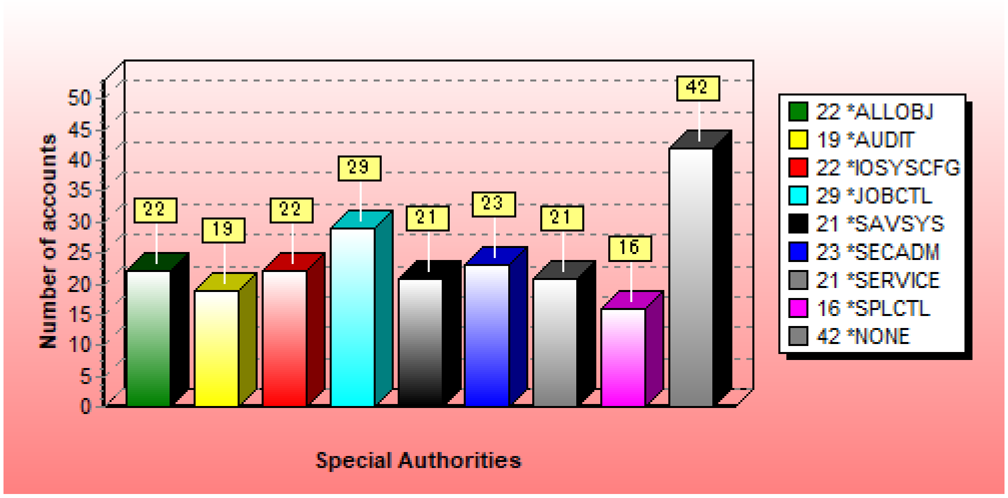
User profiles with special authorities can be misused by their legitimate users or targeted by an attacker.

Special authorities should only be used if a user or application is expected to perform a certain function that requires the special authority.

Users with *ALLOBJ authority have access to all existing objects within all directories, unless designated programs avoid it.

| Authority | Description | Total | Percent |
|---|---|---|---|
| *ALLOBJ | All object authority | 22 | 29.33 |
| *AUDIT | Audit authority | 19 | 25.33 |
| *IOSYSCFG | Input/Output system configuration | 22 | 29.33 |
| *JOBCTL | Job control authority | 29 | 38.66 |
| *SAVSYS | Save system authority | 21 | 28.00 |
| *SECADM | Security administrator authority | 23 | 30.66 |
| *SERVICE | Service authority | 21 | 28.00 |

| | | | |
|---|---|---|---|
| *SPLCTL | Spool control authority | 16 | 21.33 |
| *NONE | No authorities | 42 | 56.00 |



**Supplemental Report Reference: SRA002 - User Profile Information**

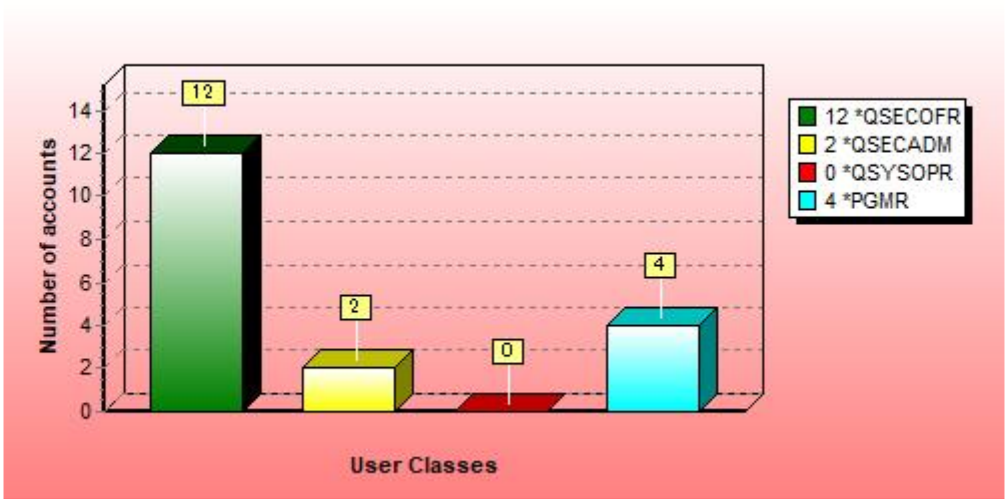
## By User Class

User class defines the role that is granted to the user. It can have the following values:

- USER (User - lowest level with very limited access)
- SYSOPR (System Operator)
- PGMR (Programmer)
- SECADM( Second Administrator - very high role)
- SECOFR (Security Officer - the highest level that has access to all, and can do everything)

User Class *SYSOPR and higher has enough power to change objects, files and system definitions. So, care should be taken in assigning these user classes. The number of users with user class *SYSOPR and higher should be considered to be reduced as much as possible, in order to eliminate the risk of improper use.

| User Class | Description | Total | Percent |
|---|---|---|---|
| *SECOFR | Security Officer | 12 | 16.00 |
| *SECADM | Second Administrator | 2 | 2.66 |
| *SYSOPR | System Operator | 0 | .00 |
| *PGMR | Programmer | 4 | 5.33 |
| | All users | 75 | |



**Supplemental Report Reference: SRA002 - User Profile Information**

## Group Profile Password Settings

✓ There are no group profile on your system that can be used to sign on and this follows recommended best practice.

**Supplemental Report Reference: SRA003 - Group Profile Password Settings**

## Default Passwords

A default password means it is the same as the user profile, therefore such profiles effectively have no password protection. Vendor-provided profiles with default passwords constitute an even greater vulnerability because they provide a way into your computer without any prior knowledge of the organization and its users.

R There are IBM profiles with default passwords on your system. 1 user profiles have default passwords of which 1 have the status of *ENABLED.

⚠ There are user-defined profiles with default passwords on your system. 7 user profiles have default passwords of which 7 have the status of *ENABLED

We recommend the following policy:

- Change password to *NONE for all user profiles starting with Q, except those required for direct signing on.
- Delete all user profiles that are not required.
- User profiles that you are not sure about, should have their password changed to *NONE.
- User profiles of users who need to sign on to the system should be given passwords that confirm to the password rules recommended in this assessment.

**Supplemental Report Reference: SRA004 - User Profiles with default password**

## Disabled Users

R There are 5 user profiles on your system that have been disabled for more than 180 days.

Disabled user profiles should be reviewed and deleted if not required. Disabling user profiles prevents their use but they represent a vulnerability because they could be enabled by mistake or by a user with malicious intent.

We recommend deleting user profiles that have been disabled beyond a reasonable period of time. 180 days is considered a reasonable period of time to allow user profiles to be disabled before deleting them. Stricter security demands might require 60 days.

**Supplemental Report Reference: SRA005 - Disabled Users**

## Inactive Users

The existence of every unnecessary user is a security vulnerability and inactive users are more often than not unnecessary. They are often users created for testing purposes or employees who have since left the organization.

We recommend deleting or disabling user profiles that have been inactive beyond a reasonable period of time. 90 days is considered a reasonable period of time to allow user profiles to be disabled before deleting them. Stricter security demands might require 45 days.

R There are 17 user profiles on your system that are enabled and have been inactive for more than 90 days.

In addition:
⚠ There are 1 user profiles on your system that are enabled and have been inactive for between 45 and 90 days.

**Supplemental Reports References:**
**SRA006 - User Profiles not used for 46 days**
**SRA007 - User Profiles not used for 61 days**
**SRA008 - User Profiles not used for 90 days**

## Limited Capability Users

Out of a total of 75 users in the system, 3 have limited capabilities, 0 are partially limited and 72 are not limited at all.

Users that are not limited can work from the command line and additionally change the initial menu, initial program, current library and attention key program. Possibly, running dangerous commands which could cause system failure.

Partially limited also allows the user to work from the command line and change the initial menu. However, it doesn't allow changing the initial program, current library or attention key program. All of these capabilities can constitute a considerable security vulnerability.

Only users with limited capabilities of *YES cannot work on the command line or change the initial menu, initial program, current library or attention key program.

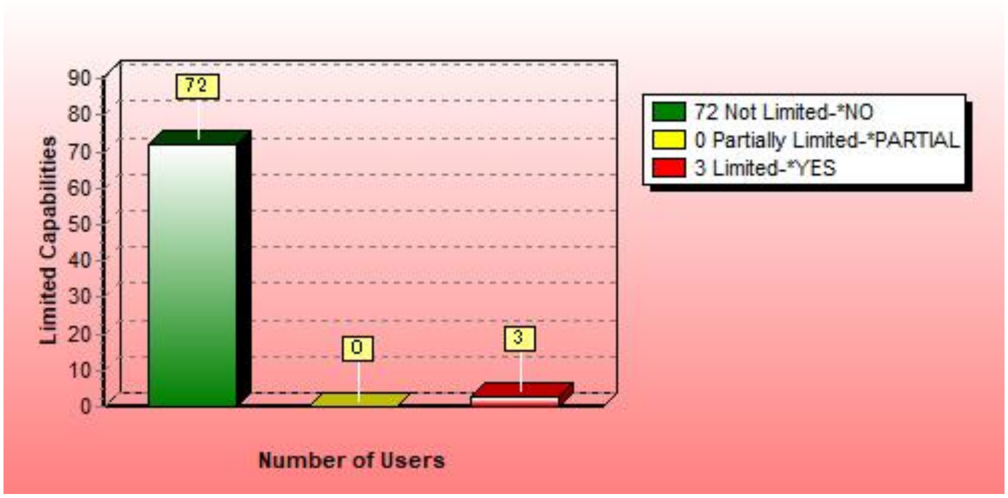
R Only 4.00% of your users are defined with limited capabilities of (*YES). We recommend defining all users in this way except those who absolutely need these capabilities.

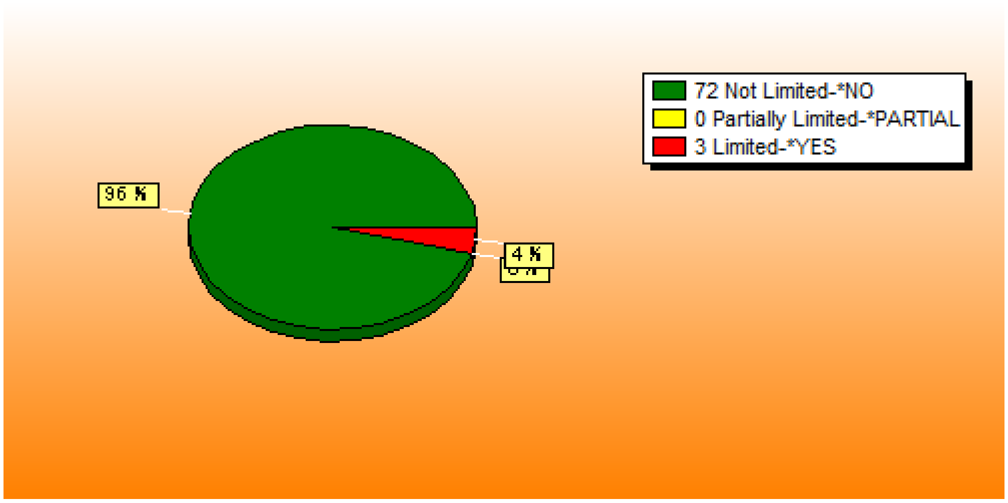
We recommend changing all user profiles to limit capabilities = *YES, except advanced system users such as operations, development and systems personnel or users who require command line access for their duties.

If you have users who require command line access, then specifying for them partially limited capabilities will

reduce the vulnerability by a small degree by not allowing changing the initial program, current library or attention key program.
You can use the WRKUSRPRF command to display all user profiles on your system and display and change as necessary.

Alternatively, you can run the user profile report type in the Enterprise Security Report Generator as a one-time or scheduled repeating task. Use Enforcive Policy Compliance module user profile template to monitor the limited capabilities parameter of your user profile with the option of manually or automatically updating the parameter for users answering to specified criteria. You can protect your system further by implementing Application Access Control to limit the remote access capabilities of users.





**Supplemental Report Reference: SRA009 - Limited Capability Users**

## Service Tools User IDs

⚠ The list of Service Tool User IDs on the system is different than the IBM shipped list. You should review these profiles on a regular basis to insure the IDs are still valid and needed for current job functions.

Service tools user IDs are user IDs that are required for accessing service functions through dedicated service tools (DST), system service tools (SST), IBM® Navigator for i (for disk unit management), and Operations Console. Service tools user IDs are created through DST or SST and are separate from IBM i user profiles. IBM provides the following service tools user IDs:

- QSECOFR
- QSRV
- 22222222
- 11111111

The service tools user IDs QSECOFR, QSRV, and 22222222 are shipped with expired default passwords and 11111111 is shipped unexpired with the default password. All service tools passwords are shipped in uppercase. You can create a maximum of 100 service tools user IDs (including the four IBM-supplied user IDs). *NOTE: A QSECOFR user profile and a QSECOFR service tools user ID are provided with every system. The QSECOFR user profile and the QSECOFR service tools user ID are not the same. They exist in different locations and are used to access different functions. Your QSECOFR service tools user ID can have a different password from your QSECOFR user profile. Service tools user IDs have different password policies from user profiles. There are two password policies available for Service Tool User IDs. The default policy is Data Encryption Standard (DES). The other password policy is Secure Hash Algorithm (SHA) which supports a longer password length and includes a larger character set. With this being the case, we recommend changing the password policy for Service Tool User IDs to SHA for an improved security policy.

**Supplemental Report Reference: SRA029 - Service Tools User IDs**

## IBM User Profiles Altered Special Authority

R There are 3 IBM supplied user profiles on your system that have been altered with increased special authorities from their default values. This is a High Risk vulnerability that should be addressed immediately. IBM supplied user profiles were designed for certain activities with specific special authorities on the system depending on the security level. Changing the account special authorities can introduce a security risk and increasing the special authority is more of a vulnerability.

**Supplemental Report Reference: SRA023 - IBM User Profiles Altered Special Authority**

## IBM Supplied Profiles with a Password

✓ No IBM supplied user profiles on your system have a password besides QSECOFR. This follows recommended best practices.

All IBM supplied user profiles (except QSECOFR) should not have a password. This is the way IBM distributes the systems with the PASSWORD parameter is set to *NONE. Any modification to this policy could be a security risk. If an IBM supplied profile is needed, the security officer should change the password temporarily for that period of time needed then change it back to *NONE.

**Supplemental Report Reference: SRA025 - IBM Supplied Profiles with a Password**

## IBM Supplied Profiles that are a Group Profile

⚠ 1 IBM supplied user profiles on your system have been assigned as group profiles on 1 user profiles. This is a vulnerability that should be addressed.

IBM supplied user profiles should not be used as a group profile. If this is done, it is giving the group members the authority of the IBM supplied profile and any of the objects the profile may have access to. This is a vulnerability which should be avoided.

**Supplemental Report Reference: SRA026 - IBM Supplied Profiles that are a Group Profile**

## User authority to IBM supplied user profiles

R Out of a total of 52 IBM-provided user profiles on the system, 9 can be used by other users. Any user who has *USE authority to an IBM user profile can submit jobs under that powerful user profile or swap into it. This is a vulnerability which could provide a higher level of security to that person without authorization. Therefore it is recommended to revoke all authorities and make the user profile its own owner. An object's owner does not require explicit authority because it has implicit authority.

**Supplemental Report Reference: SRA010 - User Authorized to IBM Supplied Profile**

## User authority to non-IBM supplied user profiles

✓ All of your non-IBM user profiles are protected from use by other users, except the object owner and power users. This is in accordance best practices.

**Supplemental Report Reference: SRA011 - User Authorized to non-IBM User Profile**

## Users Authorized to Authorization lists

⚠ There are 7 user-defined authorization lists in your system and these should be monitored periodically to ensure they are valid and up to date.

It is important to monitor authorization list members periodically to ensure they are still valid. A list of authorization lists can be produced using the authorization list report type in the Enterprise Security Report Generator. A predefined report is provided with the Report Generator, called SRA - Users Authorized to Authorization Lists. The Enterprise Security Compliance module allows you to define templates for authorization list members and authorities. The system can be automatically checked against the template for deviations and you can optionally forcefully apply the template definition to the system.

**Supplemental Report Reference: SRA021 - Users Authorized to Authorization lists**

## User Profiles with *PUBLIC not *EXCLUDE

⚠ 3 user profiles on your system have *PUBLIC authority other than *EXCLUDE. This is a vulnerability that should be addressed.

By default, the IBM i creates user profiles with *PUBLIC authority set to *EXCLUDE. It is recommended to not change this setup. If *PUBLIC is set to *USE or higher, anyone on the system can submit a job under that profile or use a job description which has that profile specified. This may let a user run jobs with a higher authority than their own.

**Supplemental Report Reference: SRA027 - User Profiles with *PUBLIC not *EXCLUDE**

## High Privilege Group Profiles

R There are 1 group profiles or supplementary groups with this authority, which is inherently granted 2 users (the total includes the Group Profiles themselves). Any users added to the group will receive this authority automatically. While this is one way of implementing special authorities to users, it requires frequent monitoring to make sure the authority is granted only to group members who really need it.

A report is provided in the Enterprise Security Report Generator, called SRA-High Privilege Group Profiles that can monitor the use of group profiles and supplementary groups. This report can be run on demand and can be scheduled to run periodically. In addition, you can use the Enforcive Compliance template to define your group profile special authority policy and check for deviations from the policy. Furthermore the template can be used to apply the policy on your system.

**Supplemental Report Reference: SRA022 - High Privilege Group Profiles**

## Job Description User Parameter

R There are 34 job descriptions with user profile name not equal *RQD defined on your system and of these, 34 can be used by anyone on the system because of *PUBLIC authority not equal *EXCLUDE. You should delete any job descriptions that are not used and set the Job Description User parameter to *RQD whenever possible.

The job description USER parameter can contain a user profile name and in some circumstances this could allow a different user to run a job that inherits the authority of the user in the USER parameter. If the system is at security level 30 or lower, a user only needs authority to the job description to run a job under the user defined in it, whereas at security level 40 and higher, a user must have authority to the job description and also to the user defined in it. It is important for systems running security level 20 and 30 to define *PUBLIC authority on the job description to *EXCLUDE. Therefore, with the exception of job descriptions required in autostart jobs or in the BCHJOB command all should have their USER parameter set to *RQD, and in cases where it is set to a user profile then authority to the job description should be carefully controlled. Restricting access to the user profile in the job description user parameter is an additional safeguard but this should not be used in place of the security measures taken at the job description level, as described above. Keep in mind if you are setting security on libraries to *PUBLIC *EXCLUDE, you should look through job descriptions to see if those libraries are listed. If they are, the users must be authorized to the library or the job will not start.

**Supplemental Report Reference: SRA032 - Job Description User Parameter**

## Object Authorities

## Library Authorities

Out of a total of 160 libraries in your system, 18 have a public authority of *EXCLUDE, 77 have a public authority of *USE, 61 libraries have authority of changing objects (*CHANGE) within the directory, and 4 are open (*ALL) to users for adding, changing or deleting any objects and also interfere with existing objects that are not sufficiently protected at the object level. This is a risk which should be reviewed.

Setting public authority to *EXCLUDE will prevent unauthorized users from adding new objects to the library in addition to preventing all access to existing objects in the library. Setting public authority to *USE will permit the use of existing objects in the library but will not permit adding objects to the library or deleting them.
In the case of objects assigned to an authorization list, public authority is taken from the authorization list only if *AUTL is specified for public authority attribute.

⚠ Some of your libraries appear to have more public authority than necessary. We suggest reviewing your libraries with public user access and change public authority to *EXCLUDE where possible The commands WRKLIB, DSPOBJAUT and RVKOBJAUT can be used to review library object authorities and change them as necessary.

**Supplemental Report Reference: SRA012 - Library Authorities**

## Commands with *PUBLIC not *EXCLUDE

R There are 7,612 commands that do not have *PUBLIC authority set to *EXCLUDE. We recommend reviewing the list and changing the appropriate ones not set to *EXCLUDE. 1,727 commands have *CHANGE or *ALL authority which are a High Risk providing open access to the public to change and/or delete the command.

By default, the IBM provides commands with a mixture of *PUBLIC authorities depending on their perceived need. Some have more authority than we would recommend. Other IBM commands may have had its authority altered which could provide *PUBLIC access. If *PUBLIC authority is set to *USE or higher, anyone on the system can have access to the command with command line or similar command entry access. This could pose a vulnerability depending on the command. 3rd Party package commands and home-grown commands could include the same *PUBLIC authority issues. So, they need to be evaluated with the same scrutiny as the IBM commands. In the case of commands assigned by an authorization list, public authority is taken from the authorization list only if *AUTL is specified for public authority attribute.

**Supplemental Report Reference: SRA028 - Commands with *PUBLIC not *EXCLUDE**

## Output Queue Authorities

⚠ Out of a total of 30 output queues on your system, 2 queue(s) allow all users authorized to the queue to display any spool file, 26 queues can be controlled by any user with operator privileges and 4 queues can have their spooled files controlled by any user with add, read and delete authority.

R Out of a total of 30 output queues on your system, 22 queue(s) can be used by any user, 1 queue(s) can be used and changed by any user and 4 queue(s) are secured from being accessed by other users.

To keep output queue data safe from unauthorized viewing and deletion, you can check output queue authority using the PRTQAUT command and then view the output produced. An alternative and more convenient method of monitoring output queue authority settings is built into the Enforcive Report Generator with the Output Queue report, which can be scheduled to run at regular intervals . A predefined report is provided with the Report Generator, called SRA - Output Queue Authorities.

**Supplemental Report Reference: SRA020 - Output Queue Authorities**

## Objects owned or accessible by Group Profile

R 8,946 objects in your system are owned by a group or supplemental group profile. This means any group member can change the objects authority and delete it. 2 users in your system are defined to automatically grant group authority to new objects they create.

We recommend not allowing objects to be owned by group profiles. There are a number of ways this can be monitored and controlled. A list of objects owned by group profiles can be produced using the object authority report type in the Enterprise security Report Generator. A predefined report called SRA - Objects Owned by Group Profile is provided in the module. A list of the users that will automatically grant object ownership to their group profiles for objects they create can be produced using the user profile report type.

The Enterprise Security Compliance module allows you to define templates for user profiles including specifying that their group profiles will not be granted authority to objects they create. The system can be automatically checked agains the template for deviations and you can optionally forcefully apply the template definition to all profiles in the system.

**Supplemental Report Reference: SRA024 - Objects owned or accessible by Group Profile**

## File Shares

⚠ 7 file shares have been defined on your system and these constitute a vulnerability as they make files in the shared directory accessible from the network.

File shares are directory paths that iSeries NetServer shares with clients PCs on the network. A file share can consist of any integrated file system directory on the IBM operating system. You can create, display, configure, and end iSeries NetServer file shares. A file share can be defined as either read-only or read/write.

Creating a file share to the root directory can cause a significant risk to your system. Sharing root ('/') exposes the whole directory structure of your entire IBM i system onto your network. If you don't have object level security set correctly, any user can map a drive on their PC and have access to any file on the system.

We recommend to monitor file shares to make sure that only the required file shares are available and their permissions are set correctly. See supplemental report SRA013 for details about the file shares defined on your system.

**Supplemental Report Reference: SRA013 - File Shares report**

## Directory Authorities

35 Directories found in your system's root directory.

R Objects in your root directory can be accessed by public users at both the object and data level.

✓ 3 directories are protected from public user access.

R 30 directories can have their data accessed by public users.

R 1 directories can be accessed by public users at both the object and data level.

The IFS file structure is a common way of communicating data with external platforms such as Windows and Unix. Allowing any kind of public authority to IFS folders severely limits your ability to protect them against unauthorized access.
Furthermore, the IFS root directory ships with *PUBLIC data authority *RWX and object authority *ALL. That means that new objects created under the root directory will inherit *PUBLIC *ALL authority and this makes them vulnerable to attacks.

Directory authorities can be monitored in Enterprise Security. A pre-defined report containing this information called "SRA-Directory Authorities Under Root" is provided in the Report Generator and the IFS Object Authority template exists in the Enterprise Security Compliance module. The template can be run to indicate deviations from policy and can be used to apply the policy to one or more directories manually or automatically.

**Supplemental Report Reference: SRA014 - Directory Authorities Under Root**

## Commands for Limited Capability Users

⚠ There are more commands with ALWLMTUSR(*YES) on the system than the ones provided by IBM though they are all in the system library. We recommend reviewing the list and changing the ones not provided by IBM back to ALWLMTUSR(*NO).

A user with limited capabilities can only run commands that are defined as being allowed to be run by limited users. The following commands are shipped by IBM with ALWLMTUSR(*YES): SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPLOBLOG, STRPCO, and WRKMSG. The combination of users with limited with limited capabilities and commands with Allow Limited User parameter only apply to running the command from the command line, the Command Entry display, FTP, REXEC, using the QCAPCMD API, or any option from a command grouping menu. It does not restrict performing the following options: Running commands from CL program that are running a command as a result of taking an option off of a menu Running remote commands through applications. If there are more commands available to a limited capability user than what IBM provides, it could allow the running of destructive commands by a person that was supposed to be setup as a limited capability user. Even worse, would be a command not in the system library which could have been created for nefarious purposes.

## Supplemental Report Reference: SRA031 - Commands for Limited Capability Users

## Programs that Adopt *ALLOBJ Authority

⚠ 28,841 programs in your system can run with a higher authority than that of the user running them. Of these, 8 programs will run with the authority of their owner rather than the user, 14,428 programs adopt authority from programs higher up in the program stack and a further 14,405 programs have both of these characteristics.

The use of adopted authority can be convenient in raising user authorization levels for specific tasks while certain programs are running. However, there is a risk of misuse of these programs and so they should be reviewed frequently.

You should identify all programs that have adopted authority from either the parameter User Profile (USRPRF) = *OWNER or User Adopted Authority (USEADPAUT) = *YES. This can be done with the WRKPGM command.

An alternative and more efficient method is to define and monitor program adopted authority and set your policy automatically using the Enforcive Compliance module, program adopted authority template.

**Supplemental Report Reference: SRA017 - Programs that adopt *ALLOBJ authority**

## Object Authorities with *PUBLIC authority

⚠ It is recommended to review all of these objects and to change as many of them as possible to *PUBLIC authority of *EXCLUDE.

It is important to review the security of objects in application libraries on a regular basis. The reason is there may be objects with unwanted access for *PUBLIC. If *PUBLIC authority is set to *USE or higher, anyone on the system can have access to that object. This could pose a vulnerability depending on the object type and use. In the case of objects authorized by an authorization list, public authority is taken from the authorization list if *AUTL is specified for the public authority attribute. It is recommended to set *PUBLIC authority to *EXCLUDE which prohibits users that are not specifically defined on the object, or authorization list in case of *AUTL, from gaining access or execution rights. Proceed with caution because a change in object authority may affect applications. Consult with software providers in case you have third party applications.

**Supplemental Report Reference: SRA030 - Object Authorities with *PUBLIC authority report shows public authority settings for *FILE, *PGM and *CMD object types**

## Access through Network

## Open Ports

⚠ There are 38 ports in listening mode on your system. Each of these ports has a service that is running and handling requests sent to the port. It is therefore important to know which service is listening at each port. Without reviewing this regularly, unwanted and even potentially harmful applications may be active and running on your system.

Ports that are not meant to be in use can, if not protected, be used by hackers as 'backdoors' into the system. Required ports should be monitored and protected against improper use. The status of your ports should be investigated at regular intervals to ensure that those in listening mode are communicating with programs that are known and meant to be active. One way of doing this is with the NETSTAT command and displaying the port numbers on the connection status screen. A more efficient way is to use the Enforcive Policy Compliance module to define and check a policy for listening ports, or to use the Report Generator Open Ports report, for which there is a predefined report called SAR - Open Ports. The Enforcive Firewall contains several functions to add security at the port level including prevention of a range or collection of ports from being opened, sources of prevention of connecting to a port from within the IBM i, by user and sources of access from else in the network to IBM i ports. Enterprise Security Application Access Control hardens the ports that need to be in use by limiting their use to certain users and applications.

The ports that are currently in listening mode are listed in the table below:

| Port Id | Description | User |
|---|---|---|
| 21 | ftp-control | QTCP |
| 23 | telnet | QTCP |
| 25 | smtp | QTCP |
| 389 | ldap | QDIRSRV |
| 427 |  | QSYS |
| 427 |  | QSYS |
| 446 | drda | QUSER |
| 447 | ddm | QUSER |
| 448 | ddm-ssl | QUSER |
| 449 | as-svrmap | QUSER |
| 515 | lpd | QTCP |
| 657 | rmc | QSYS |
| 992 | telnet-ssl | QTCP |
| 3000 | as-sts | QSRV |
| 4800 |  | QSYS |
| 4800 |  | QSYS |
| 5544 | as-mgtctrlj | QYPSJSVR |
| 5555 | as-mgtctrl | QYPSJSVR |
| 8014 |  | QTMHHTTP |
| 8015 |  | QTMHHTTP |
| 8470 | as-central | QUSER |
| 8471 | as-database | QUSER |
| 8472 | as-dtaq | QUSER |
| 8473 | as-file | QUSER |
| 8474 | as-netprt | QUSER |
| 8475 | as-rmtcmd | QUSER |
| 8476 | as-signon | QUSER |
| 8477 | as-netdrive | QUSER |
| 8478 | as-transfer | QUSER |
| 8479 | as-vrtprint | QUSER |
| 9470 | as-central-s | QUSER |
| 9471 | as-database-s | QUSER |
| 9472 | as-dtaq-s | QUSER |
| 9473 | as-file-s | QUSER |
| 9474 | as-netprt-s | QUSER |
| 9475 | as-rmtcmd-s | QUSER |
| 9476 | as-signon-s | QUSER |

| | | |
|---|---|---|
| 10002 | | QTMHHTTP |

**Supplemental Report Reference: SRA015 - Open Ports**

## Exit Programs

⚠ The system Exit Points are listed in the table below. The Work with Registration Information Command (WRKREGINF) shows information about exit points and exit programs. Information about a single exit point, multiple exit points and the exit programs associated with the exit points are displayed. The command is similar to the Retrieve Exit Information (QUSRTVEI) Application Programming Interface (API).

- The name of the Exit Point and Description are provided.
- The "Allow Deregister" parameter determines whether or not the exit point can be deregistered (removed from the registration facility repository). This value is set when the exit point is registered and cannot be changed. Having a value of *YES is a concern being that this allows the deregistering of the Exit Point.
- The "Allow Change" parameter determines whether or not the exit point values shown on this display can be changed. When no change is specified, the only way to change the exit point values is to deregister the exit point, reregister the exit point, and add the exit programs again. Having a value of *YES is a concern being that this allows for easily changing exit point information without deregistering of the Exit Point.
- The Number of Exit Programs parameter is the current number of exit programs associated with this exit point. This lets you know if there are Exit Programs connected to this Exit Point.

Having network servers active introduces multiple risks of those servers being compromised. This may allow remote access to your system, objects, and files without an audit log or security checking in place depending on your object level security settings. The network related Exit Programs are a great way to provide additional level of protection and monitoring for the network servers. There are several third party solutions available in the market , such as Enforcive Enterprise Security suite, that provides the exit program security and monitoring solutions. You should also check Exit Points with Exit Programs to insure you know who created it and why it is in place. It is possible to have programs in place which may cause system degradation or provide sensitive information to unwanted sources.

The Exit Programs are listed in the table below:

| Exit Point | Description | Allow Deregister | Allow Change | Number of Exit Programs |
|---|---|---|---|---|
| QIBM_QCA_CHG_COMMAND | Cambiar programas de salida de mandato | *NO | *NO | 0 |
| QIBM_QCA_RTV_COMMAND | Recuperar programas de salida de mandato | *NO | *NO | 5 |
| QIBM_QCST_ADMDMN | Soporte del dominio de administración de clúster | *NO | *NO | 8 |
| QIBM_QCST_ADMDMN | Soporte del dominio de administración de clúster | *NO | *NO | 17 |
| QIBM_QCST_CLU | Soporte de nodo de clúster | *NO | *NO | 0 |
| QIBM_QCST_CRG | Soporte de grupo de recurso de clúster | *NO | *NO | 0 |
| QIBM_QC3_CLR_MSTKEY | Borrar clave maestra | *NO | *NO | 0 |
| QIBM_QC3_DLT_KREC | Suprimir registro de clave | *NO | *NO | 0 |
| QIBM_QC3_SET_MSTKEY | Establecer clave maestra | *NO | *NO | 0 |
| QIBM_QC3_TRN_KSF | Traducir almacén de claves | *NO | *NO | 0 |
| QIBM_QDB_CLOSE | Cerrar pgm de salida de archivo de base de datos | *NO | *NO | 0 |

|  |  |  |  |  |
|---|---|---|---|---|
| QIBM_QDB_OPEN | Pgm salida apertura arch base de datos | *NO | *NO | 0 |
| QIBM_QDC_VRYEXIT | Punto de salida de preproceso para desactivar conf | *NO | *NO | 0 |
| QIBM_QDC_VRYEXIT | Punto de salida de preproceso para desactivar conf | *NO | *NO | 0 |
| QIBM_QDC_VRYEXIT | Punto de salida de preproceso para desactivar conf | *NO | *NO | 0 |
| QIBM_QDC_VRYEXIT | Punto de salida de preproceso para desactivar conf | *NO | *NO | 0 |
| QIBM_QHQ_DTAQ | Servidor de colas de datos original | *NO | *YES | 0 |
| QIBM_QIMG_TRANSFORMS | Punto de salida para transformaciones de impresión | *NO | *YES | 0 |
| QIBM_QJO_CHG_JRNRCV | Cambiar receptor de diario | *NO | *NO | 0 |
| QIBM_QJO_DLT_JRNRCV | Suprimir receptor de diario | *YES | *YES | 0 |
| QIBM_QLZP_LICENSE | Servidor de gestión de licencias original | *NO | *YES | 0 |
| QIBM_QMF_MESSAGE | Servidor de mensajes original | *NO | *YES | 0 |
| QIBM_QMH_HDL_INQEXT | Manejar consulta a *EXT | *NO | *NO | 0 |
| QIBM_QMH_REPLY_INQ | Manejar respuesta a mensajes de consulta | *NO | *NO | 0 |
| QIBM_QMO_OPT | Texto no disponible para el mensaje CPX2BC0 archiv | *NO | *NO | 0 |
| QIBM_QNM_EVENT_DTAQ | Notificación de eventos de red | *NO | *NO | 0 |
| QIBM_QNPS_ENTRY | Servidor de impresión de red - entrada | *NO | *YES | 0 |
| QIBM_QNPS_SPLF | Servidor de impresión de red - archivo de spool | *NO | *YES | 0 |
| QIBM_QOE_OV_USR_ADM | Administración OfiVisión/400 | *NO | *YES | 0 |
| QIBM_QOE_OV_USR_SND | Salida de Envío de Correo OfiVisión/400 | *NO | *YES | 0 |
| QIBM_QOK_NOTIFY | Punto salida notificación a directorio sistema | *NO | *NO | 0 |
| QIBM_QOK_SUPPLIER | Punto salida suministrador directorio sistema | *NO | *NO | 0 |
| QIBM_QOK_VERIFY | Punto salida verificación directorio sistema | *NO | *NO | 0 |
| QIBM_QPA_DEVSEL | Selección de dispositivo virtual | *NO | *NO | 0 |
| QIBM_QPMW_ARM4_ADAP | Programa de salida de adaptador ARM | *NO | *NO | 0 |
| QIBM_QPQ_TRANSFORM | Punto de salida de transformación de IPDS en PDF | *YES | *YES | 0 |
| QIBM_QPWFS_FILE_SERV | Servidor de archivos | *NO | *NO | 0 |
| QIBM_QP0L_SCAN_CLOSE | Explorar sistema de archivos integrado al cerrar | *NO | *NO | 0 |
| QIBM_QP0L_SCAN_OPEN | Explorar sistema de archivos integrado al abrir | *NO | *NO | 0 |
| QIBM_QQQ_QUERY_GOVR | QUERY GOVERNOR | *NO | *NO | 0 |
| QIBM_QRQ_SQL | Servidor SQL remoto original | *NO | *YES | 0 |
| QIBM_QSO_ACCEPT | Punto de salida para APIs con conexiones socket | *NO | *NO | 0 |

| | | | | |
|---|---|---|---|---|
| QIBM_QSO_CONNECT | Punto de salida para API connect() sockets | *NO | *NO | 0 |
| QIBM_QSO_LISTEN | Punto de salida para API listen() sockets | *NO | *NO | 0 |
| QIBM_QSP_SECURITY | Punto de salida de seguridad de archivo en spool | *NO | *NO | 0 |
| QIBM_QSP_SECURITY | Punto de salida de seguridad de archivo en spool | *NO | *NO | 0 |
| QIBM_QSP_SPLF_LSTACT | Acc. de lista arch spool def por usuar | *NO | *NO | 0 |
| QIBM_QSQ_CLI_CONNECT | CLI connection exit point | *NO | *NO | 0 |
| QIBM_QSU_ALW_EDIT | EXIT POINT FOR SEU USER TO PREVENT EDITING | *YES | *NO | 0 |
| QIBM_QSU_LCMD | EXIT POINT FOR SEU USER DEFINE LINE COMMANDS | *YES | *NO | 0 |
| QIBM_QSY_CERT_APPS | Aplicaciones que utilizan certificados | *NO | *NO | 29 |
| QIBM_QSY_CHG_PROFILE | Cambiar perfil de usuario - después del cambio | *NO | *NO | 1 |
| QIBM_QSY_CHG_PROFILE | Cambiar perfil de usuario - después del cambio | *NO | *NO | 0 |
| QIBM_QSY_CHK_PASSWRD | Comprobar contrase¦a | *NO | *NO | 0 |
| QIBM_QSY_CRT_PROFILE | Crear perfil de usuario | *NO | *NO | 1 |
| QIBM_QSY_DLT_PROFILE | Suprimir perfil de usuario - después de supresión | *NO | *NO | 4 |
| QIBM_QSY_DLT_PROFILE | Suprimir perfil de usuario - después de supresión | *NO | *NO | 0 |
| QIBM_QSY_HOSTFUNC | Funciones de sistema principal | *NO | *NO | 56 |
| QIBM_QSY_OPNAVCENTRL | Funciones centrales de Navigator | *NO | *NO | 0 |
| QIBM_QSY_OPNAVCLIENT | Funciones locales de Navigator | *NO | *NO | 0 |
| QIBM_QSY_OTHERCENTRL | Funciones centrales de otros clientes | *NO | *NO | 0 |
| QIBM_QSY_OTHERCLIENT | Funciones locales de otros clientes | *NO | *NO | 0 |
| QIBM_QSY_RST_PROFILE | Restaurar perfil de usuario | *NO | *NO | 0 |
| QIBM_QSY_VLD_PASSWRD | Validar contrase¦a CHGPWD, QSYCHGPW | *NO | *NO | 0 |
| QIBM_QSY_VLD_PASSWRD | Validar contrase¦a CHGPWD, QSYCHGPW | *NO | *NO | 0 |
| QIBM_QTF_TRANSFER | Función de transferencia de archivos original | *NO | *YES | 0 |
| QIBM_QTG_DEVINIT | Inicialización de dispositivo Telnet. | *NO | *NO | 0 |
| QIBM_QTG_DEVTERM | Terminación de dispositivo Telnet. | *NO | *NO | 0 |
| QIBM_QTMF_CLIENT_REQ | Validación de petición de cliente FTP | *YES | *NO | 0 |
| QIBM_QTMF_SERVER_REQ | Validación de petición de servidor FTP | *YES | *NO | 0 |
| QIBM_QTMF_SVR_LOGON | Inicio de sesión del servidor FTP | *YES | *NO | 0 |
| QIBM_QTMF_SVR_LOGON | Inicio de sesión del servidor FTP | *YES | *NO | 0 |
| QIBM_QTMF_SVR_LOGON | Inicio de sesión del servidor FTP | *YES | *NO | 0 |
| QIBM_QTMX_SERVER_REQ | Validación de petición del servidor REXEC | *YES | *NO | 0 |

|  |  |  |  |  |
|---|---|---|---|---|
| QIBM_QTMX_SVR_LOGON | Inicio de sesión del servidor REXEC | *YES | *NO | 0 |
| QIBM_QTMX_SVR_LOGON | Inicio de sesión del servidor REXEC | *YES | *NO | 0 |
| QIBM_QTMX_SVR_SELECT | Selección de proceso de mandato de servidor REXEC | *YES | *NO | 0 |
| QIBM_QTOD_DHCP_ABND | Notificación de enlace de direcciones DHCP | *YES | *YES | 0 |
| QIBM_QTOD_DHCP_ARLS | Notificación de liberación de direcciones DHCP | *YES | *YES | 0 |
| QIBM_QTOD_DHCP_REQ | Validación de paquetes de peticiones DHCP | *YES | *NO | 0 |
| QIBM_QTOD_SERVER_REQ | Validación de petición del servidor TFTP | *YES | *YES | 0 |
| QIBM_QVP_PRINTERS | Servidor de impresión virtual original | *NO | *YES | 0 |
| QIBM_QWC_JOBITPPGM | Punto de salida de programa de interrup de trab | *NO | *NO | 0 |
| QIBM_QWC_PRERESTRICT | ENDSYS ENDSBS *ALL Punto de salida de proceso de e | *NO | *NO | 0 |
| QIBM_QWC_PWRDWNSYS | Punto de salida de preapagado del sistema | *NO | *NO | 0 |
| QIBM_QWC_PWRDWNSYS | Punto de salida de preapagado del sistema | *NO | *NO | 0 |
| QIBM_QWC_QSTGLOWACN | Acción de límite inferior almacenamiento auxiliar | *NO | *NO | 0 |
| QIBM_QWC_RESUME | Reanudar el sistema | *NO | *NO | 0 |
| QIBM_QWC_SUSPEND | Suspender sistema | *NO | *NO | 0 |
| QIBM_QWT_JOBNOTIFY | Notificación de trabajo | *NO | *NO | 2 |
| QIBM_QWT_PREATTNPGMS | Punto de salida de programa de preatención | *NO | *NO | 0 |
| QIBM_QWT_SYSREQPGMS | Punto salida programa petición presistema | *NO | *NO | 0 |
| QIBM_QYIV_INVGTRSRV | Servicios de recogida de inventario | *NO | *NO | 0 |
| QIBM_QYIV_INVPRCSRV | Servicios de proceso de inventario | *NO | *NO | 0 |
| QIBM_QYME_MONITOR | Mandatos de umbral de Management Central | *YES | *YES | 0 |
| QIBM_QZCA_ADDC | A¦adir punto de salida de Cliente | *YES | *YES | 0 |
| QIBM_QZCA_REFC | Renovar punto de salida de Información de Cliente | *YES | *YES | 0 |
| QIBM_QZCA_RMVC | Eliminar punto de salida de Cliente | *YES | *YES | 0 |
| QIBM_QZCA_SNMPTRAP | Punto de salida de direccionamiento de detección S | *YES | *YES | 0 |
| QIBM_QZCA_UPDC | Actualizar punto de salida de Información de Clien | *YES | *YES | 0 |
| QIBM_QZDA_INIT | Servidor de base de datos - entrada | *NO | *YES | 0 |
| QIBM_QZDA_NDB1 | Servidor de base de datos - acceso base de datos | *NO | *YES | 0 |
| QIBM_QZDA_NDB1 | Servidor de base de datos - acceso base de datos | *NO | *YES | 0 |
| QIBM_QZDA_ROI1 | Servidor de base de datos - información de objeto | *NO | *YES | 0 |
| QIBM_QZDA_ROI1 | Servidor de base de datos - información de objeto | *NO | *YES | 0 |

| | | | | |
|---|---|---|---|---|
| QIBM_QZDA_SQL1 | Servidor de base de datos - Acceso SQL | *NO | *YES | 0 |
| QIBM_QZDA_SQL2 | Servidor de base de datos - Acceso SQL | *NO | *YES | 0 |
| QIBM_QZHQ_DATA_QUEUE | Servidor de colas de datos | *NO | *YES | 0 |
| QIBM_QZMFMSF_ACT | Salida de contabilidad MSF | *NO | *NO | 1 |
| QIBM_QZMFMSF_ADR_RSL | Resolución de direcciones MSF | *NO | *NO | 3 |
| QIBM_QZMFMSF_ATT_CNV | Conversión de anexos MSF | *NO | *NO | 2 |
| QIBM_QZMFMSF_ATT_MGT | Gestión de conexiones MSF | *NO | *NO | 2 |
| QIBM_QZMFMSF_ENL_PSS | Proceso de sobres MSF | *NO | *NO | 1 |
| QIBM_QZMFMSF_LCL_DEL | Entrega local MSF | *NO | *NO | 4 |
| QIBM_QZMFMSF_LST_EXP | Ampliación de listas MSF | *NO | *NO | 2 |
| QIBM_QZMFMSF_MSG_FWD | Reenvío de mensajes MSF | *NO | *NO | 3 |
| QIBM_QZMFMSF_NON_DEL | MSF no entregados | *NO | *NO | 3 |
| QIBM_QZMFMSF_SEC_AUT | Seguridad y autorización de MSF | *NO | *NO | 1 |
| QIBM_QZMFMSF_TRK_CHG | Seguimiento de cambios de mensajes de correo MSF | *NO | *YES | 0 |
| QIBM_QZMFMSF_VLD_TYP | Tipo de validación MSF | *NO | *NO | 0 |
| QIBM_QZRC_RMT | Llamada a programa/mandato Remoto | *NO | *YES | 0 |
| QIBM_QZSC_LM | Servidor central - gestión de licencias | *NO | *YES | 0 |
| QIBM_QZSC_NLS | Servidor central - mapa de conversiones | *NO | *YES | 0 |
| QIBM_QZSC_SM | Servidor central - gestión de clientes | *NO | *YES | 0 |
| QIBM_QZSO_SIGNONSRV | Servidor inicio sesión TCP | *NO | *YES | 0 |

**Supplemental Report Reference: SRA016 - Exit Programs**

# Conclusion

This concludes the findings of all 57 security definition checks made on system S21D162V on 2019-07-19, which together should give a picture of the degree of risk to which your IBM i is exposed.

Recommended Action:
After reviewing the findings at the management summary and checking detail levels, make changes where possible to your system definitions and rerun the assessment tool. You should repeat this process at frequent intervals to ensure that the impact of any system changes that might have been made since last checked is known and documented.