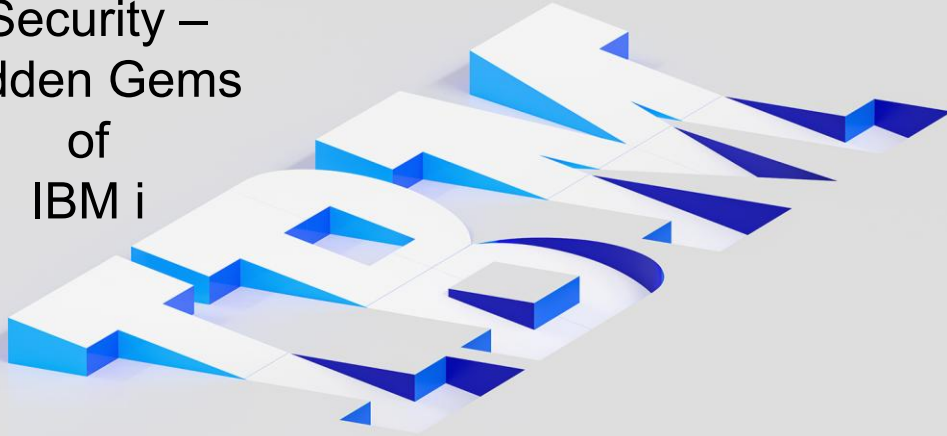


Security – Hidden Gems of IBM i



Scott Forstie
Db2 for i Business Architect

Carol Woodbury
IBM i Security SME and Senior Advisor

© 2026 International Business Machines Corporation

IBM i

1

Security – Hidden Gems of IBM i

A “Hidden Gem” is an IBM i feature, technology, or wisdom that might be unknown to you

To be considered a “Gem”, the topic needs to provide value

The focus of this Hidden Gems session is Security



© Copyright IBM Corporation 2026

2

Security – Hidden Gems of IBM i

A “Hidden Gem” is an IBM i feature, technology, or wisdom that might be unknown to you

To be considered a “Gem”, the topic needs to provide value

The focus of this Hidden Gems session is Security

Yes... Security can be fun



© Copyright IBM Corporation 2026

3

Security – Hidden Gems of IBM i

A “Hidden Gem” is an IBM i feature, technology, or wisdom that might be unknown to you

To be considered a “Gem”, the topic needs to provide value

The focus of this Hidden Gems session is Security

Yes... Security can be fun

Just kidding... Security is rarely fun



© Copyright IBM Corporation 2026

4

Do NOT Share Secrets!



© 2026 International Business Machines Corporation

5

5

SQL Obfuscation



6

Obfuscate your SQL PL

SQL Functions and Procedures

QSYS2.SYSROUTINES includes the **ROUTINE_DEFINITION** column:

ROUTINE_DEFINITION	ROUTINEDEF	DBCLOB(2M) 13488	CCSID	If this is an SQL routine, this column contains the SQL routine body.
		Nullable		If this is an obfuscated routine, the text starts with the WRAPPED keyword and is followed by the encoded form of the statement text.
				Contains the null value if this is not an SQL routine.

Is your routine source available for anyone to query?

7

Obfuscate your SQL PL

SQL Triggers

QSYS2.SYSTRIGGERS includes the **ACTION_STATEMENT** column:

ACTION_STATEMENT	TEXT	DBCLOB(2097152) 13488	CCSID	Text of the SQL statements in the trigger action.
		Nullable		If this is an obfuscated trigger, the text starts with the WRAPPED keyword and is followed by the encoded form of the statement text.
				Contains the null value if this is a trigger created via the ADPPFTRG command.

Is your trigger source available for anyone to query?

8

Trigger Source

```
SELECT trigger_schema, trigger_name, action_statement
FROM qsys2.systriggers
WHERE action_statement IS NOT null
AND action_statement NOT LIKE 'WRAPPED QSQ%'
ORDER BY trigger_schema;
```

TRIGGER_SCHEMA	TRIGGER_NAME	ACTION_STATEMENT
ARCAD_DTA	ORD701_INSERT_ORDER	BEGIN UPDATE HSBC01_DTA . CUSTOMER SET CULAS
BRANCH_OFFICE_099	CUSTOMERS_TRIGGER	BEGIN ATOMIC DECLARE OPERATION VARCHAR (10) FI
HSCOMMOND2	INSERTITEM	BEGIN ATOMIC INSERT INTO HSRRRPG . ITEMBAS (ITI
HSCOMMON10	REPLACE_MASK_BIRTHDAY	BEGIN IF INSERTING THEN SET N . BIRTHDAY = DEFAI
HSCOMMON10	INSERTITEM	BEGIN ATOMIC INSERT INTO HSCOMMON10 . ITEMBAS (
HSCOMMON10	TRGAGGSTCK	BEGIN DECLARE XITEMNO INTEGER DEFAULT 0 ; DECLAI

9

Obfuscate your SQL PL

```
--
-- Generate Obfuscated SQL PL
--
VALUES(SYSIBMADM.WRAP
('CREATE PROCEDURE chgSalary(IN empno CHAR(6))
BEGIN
UPDATE employee SET empsal = empsal*(1 + .05*empjobtype)
WHERE empid = empno;
END') );
```



```
CREATE PROCEDURE CHGSALARY ( IN EMPNO CHAR ( 6 ) )
WRAPPED QSQ07040 aacxW8p1W8VnG8pHG8VnG8pD68:r69pn19VB08FJWqpdW8pdW8pdW_FHqeba
qebaJq:otqQkPPBKTfu8somid1ZxRePVWQ:bE_S1IHeV01CU5AvdG231KqJ04aGHWEpniJI4Ud9UCK97
KHedXzi1gmKGgB7nT4kD2cxNS7wUjsNE:CkSI10796bdylzFfhg3xvXT14qaa;
```

10

SQL PL and Obfuscation

```
call SYSIBMADM.CREATE_WRAPPED('CREATE PROCEDURE prodlib.chgSalary(IN empno CHAR(
6))
BEGIN
  UPDATE employee SET empsal = empsal*(1 + .05*empjobtype)
  WHERE empid = empno;
END');
```

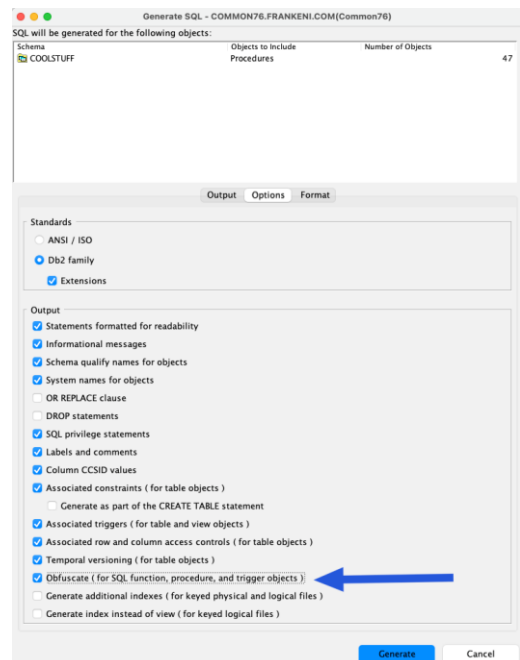
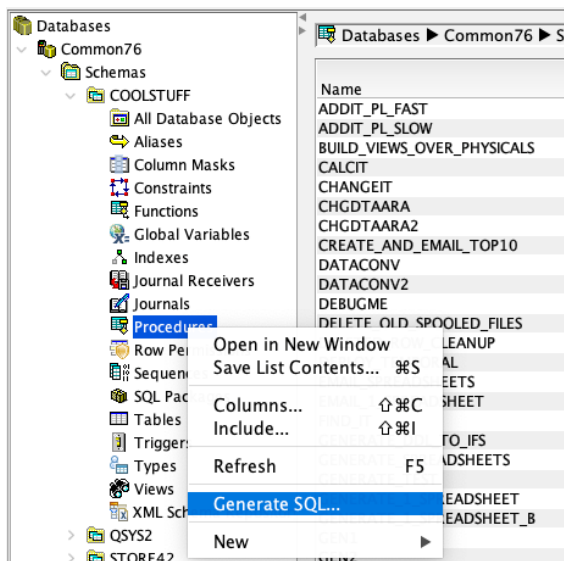
```
select routine_definition from qsys2.sysroutines
where routine_schema = 'PRODLIB';
```



```
ROUTINE_DEFINITION
WRAPPED QSQ07040 aacxw8p1w8VnG8pHG8VnG8pD69pn69FL19FpY9FpWqpdw
```

11

Generate SQL



12

SQL Routines – Not Obfuscated

```
SELECT routine_schema, routine_type,
       COUNT(*) AS unprotected_count
FROM qsys2.sysroutines
WHERE routine_definition IS NOT null
      AND routine_definition NOT LIKE 'WRAPPED QSQ%'
GROUP BY routine_schema, routine_type
ORDER BY routine_schema;
```

ROUTINE_SCHEMA	ROUTINE_TYPE	UNPROTECTED_COUNT
CAROLNEW	PROCEDURE	1
COOLSTUFF	PROCEDURE	48
COOLSTUFF	FUNCTION	43
DAWNM	PROCEDURE	4

13

SQL Triggers – Not Obfuscated

```
SELECT trigger_schema, COUNT(*) AS unprotected_count
FROM qsys2.systriggers
WHERE action_statement IS NOT null
      AND action_statement NOT LIKE 'WRAPPED QSQ%'
GROUP BY trigger_schema
ORDER BY trigger_schema;
```

TRIGGER_SCHEMA	UNPROTECTED_COUNT
ARCAD_DTA	1
BRANCH_OFFICE_099	1
HSCCOMMOND2	1
HSCCOMMON10	4

14

Secure Columns



15

Db2 for i Tooling

Db2 for i includes some incredibly powerful & helpful tools!

- Visual Explain
- SQL Performance Monitor
- SQL Plan Cache – Snapshot
- SQL Plan Cache – Event Monitor
- SQL Plan Cache – Show Statements
- SQL Details for Jobs



Enlightening

16

Db2 for i Tooling

Db2 for i includes some incredibly powerful & helpful tools!

- Visual Explain
- SQL Performance Monitor
- SQL Plan Cache – Snapshot
- SQL Plan Cache – Event Monitor
- SQL Plan Cache – Show Statements
- SQL Details for Jobs



Dangerous

Security Topic:

Should the user of these tools see the literal values provided for all columns?

```
SELECT *
FROM toystore.employee
WHERE ssn = '331442553';
```

© 2026 International Business Machines Corporation

17

17

SET_COLUMN_ATTRIBUTES

This procedure allows you to change the attributes of a column such that the value ***SECURE** will appear instead of the literal value used for the column when using Db2 for i tooling to examine the SQL statement

The default for this topic is **SECURE NO**

If the user is the QSECOFR user profile, this protection does not apply

```
--
-- Prevent the SSN values from surfacing thru Db2 for i tooling
--
CALL sysproc.set_column_attribute('TOYSTORE', 'EMPLOYEE', 'SSN', 'SECURE YES');
```

<https://www.ibm.com/docs/en/i/7.6.0?topic=services-set-column-attribute-procedure>

© 2026 International Business Machines Corporation

18

18

SYSCOLUMNS2

The SYSCOLUMNS2 catalog shows whether columns have been secured

```
--
-- Which columns have been secured?
--
SELECT column_name, secure,
       CASE
         WHEN secure THEN TRUE
         ELSE FALSE
       END secured
FROM   qsys2.syscolumns2
WHERE  table_name = 'EMPLOYEE' AND table_schema = 'TOYSTORE';
```

COLUMN_NAME	SECURE	SECURED
SALARY	0	false
BONUS	0	false
COMM	0	false
SSN	1	true

© 2026 International Business Machines Corporation

19

19

Secured Column

The screenshot shows the 'SQL Plan Cache Statements' tool interface. On the left, there are various filters to apply, such as 'Minimum runtime for the longest execution of the statement' and 'Statements that ran on or after this date and time'. The main area displays a table of statements with columns: Last Time Run, Most Expensive Time (sec), Total Processing Time (sec), Total Times Run, Average Processing Time (sec), and Statement. A context menu is open over the selected statement, showing options like 'Visual Explain', 'Show Longest Runs', 'Work with SQL Statement and Variables', and 'Plan'.

Last Time Run	Most Expensive Time (sec)	Total Processing Time (sec)	Total Times Run	Average Processing Time (sec)	Statement
2026-04-11 12:29:07.480030	0.0000	0.0000	2	0.0001	SELECT * FROM toyst

© 2026 International Business Machines Corporation

20

20

Secured Column

The screenshot shows the 'SQL Plan Cache Statements' interface for 'COMMON76.FRANKENI.COM(Common76)'. The 'Filters applied' section shows 'Statements that reference these objects: toystore.employee'. A table lists the statements, with the first entry highlighted:

Last Time Run	Most Expensive Time (sec)	Total Processing Time (sec)	Total Times Run	Average Processing Time (sec)	Statement
2026-04-11 12:29:07.480030	0.0000	0.0000	2	0.0001	SELECT * FROM toyst

A context menu is open over the statement, with 'Work with SQL Statement and Variables' selected. A blue arrow points from this menu to a code editor window showing the following SQL query:

```

1 SELECT *
2 FROM toystore.employee
3 WHERE ssn = '*SECURE'

```

The code editor window title is 'Production - Be Careful - Run SQ'. The interface also shows various filter options on the left, such as 'Minimum runtime for the longest execution of the statement' and 'Statements that ran on or after this date and time'.

© 2026 International Business Machines Corporation

21

Changing Database File Authorizations in Production



© Copyright IBM Corporation 2026

22

How do you change Permissions on a DB file in Production?

Use an Authorization list, of course!!!

You can always change the authority to the list, even if the file is in use.

© 2026 International Business Machines Corporation

23

23

Changing Database File Authorizations Production

```
grant all on table toystore.employee to timmr;  
revoke all on table toystore.employee from timmr;
```

© 2026 International Business Machines Corporation

24

Changing Database File Authorizations Production

```
grant all on table toystore.employee to timmr;
revoke all on table toystore.employee from timmr;
```

```
grant all on table toystore.employee to timmr
✘ SQL State: 57033
Vendor Code: -913
Message: [SQL0913] Row or object EMPLOYEE in TOYSTORE type *FILE in use.
```

Granting or Revoking Authorities requires an EXCLUSIVE LOCK on the *FILE object

© 2026 International Business Machines Corporation

25

Break the Rules

```
call qsys2.override_qaqqini(1);
call qsys2.override_qaqqini(2,
                          'ALLOW_DDL_CHANGES_WHILE_OPEN',
                          '*YES');
```

```
call qsys2.override_qaqqini(2, 'ALLOW_DDL_CHANGES_WHILE_OPEN', '*YES')
✓ Return Code = 0
✓ Statement ran successfully (77 ms)
```

[04/19/2026, 07:37:19 PM] Run Selected...

```
grant all on table toystore.employee to timmr
✓ Statement ran successfully (113 ms)
```

<https://www.ibm.com/support/pages/allowddlchangeswhileopen-qaqqini-option>

© 2026 International Business Machines Corporation

26

ALLOW_DDL_CHANGES_WHILE_OPEN

ALLOW_DDL_CHANGES_WHILE_OPEN applies to these SQL statements:

- GRANT
- REVOKE

And to these CL commands:

- Grant Object Authority (GRTOBJAUT)
- Revoke Object Authority (RVKOBJAUT)

<https://www.ibm.com/support/pages/allowddlchangeswhileopen-qaqqini-option>

© 2026 International Business Machines Corporation

27

OVERRIDE_QAQQINI procedure

```
call qsys2.override_qaqqini(1);
-- Create the QAQQINI override file within the QTEMP library

call qsys2.override_qaqqini(2,
                             <QAQQINI name>,
                             <QAQQINI value>);
-- Set a QAQQINI option to the specified value
-- See QAQQINI query options for the list of options

call qsys2.override_qaqqini(3);
-- Discard the temporary QAQQINI file
```

<https://www.ibm.com/docs/en/i/7.6.0?topic=services-override-qaqqini-procedure>

© 2026 International Business Machines Corporation

28

Saving Private Authorities without a SAVSECDTA



© Copyright IBM Corporation 2026

29

Save / Restore Private Authorities with an Object

Save Object (SAV0BJ)

Type choices, press Enter.

```

Private authorities . . . . . *NO      *NO, *YES
Storage . . . . . *KEEP      *KEEP, *OFF
Data compression . . . . . *DEV      *DEV, *OFF
Data compaction . . . . . *DEV      *DEV, *OFF
Libraries to omit . . . . . *NONE
+ for more values
Objects to omit:
  Object . . . . . Name, g
  Library . . . . . *ALL      Name, g
  Object type . . . . . *ALL      *ALL, *
+ for more values
ASP device . . . . . *          Name, *
Output . . . . . *NONE      *NONE,
File to receive output . . . . . Name
Library . . . . . *LIBL      Name, *
          
```

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How
F24=More keys
Messages pending on other displays.

Restore Object (RST0BJ)

Type choices, press Enter.

```

File member:
  File . . . . . *ALL      Name, *ALL
  Member . . . . . *ALL      Name, generic*, *ALL, *NONE
+ for more values
Data base member option . . . . *MATCH *MATCH, *ALL, *NEW, *OLD
Defer ID . . . . . *NONE      Name, *NONE
Spooled file data . . . . . *NEW      *NEW, *NONE
Private authorities . . . . . *NO      *NO, *YES
          
```

Date when sav
Time when sav
Allow object : Specifies whether to restore private authorities with the objects that are restored.

Force object
Convert dur
Objects to : More...

F3=Exit F4= F2=Extended help F10=Move to top F12=Cancel
F24=More keys F13=Information Assistant F20=Enlarge F24=More keys

Messages pend

© 2026 IBM Corporation

30

30

Accidental Adopted Authority



© Copyright IBM Corporation 2026

31

Protections against Privilege Escalation

When a program adopts authority, it uses the authority for the user that is running **plus** the authority of the owner of the executable



The **adopted authority** is in affect while the program is on the call stack

The USRPRF(*OWNER vs *USER) parameter indicates whether adopted authority will be used when the program is called

Reference documentation - [Objects that adopt the owner's authority](#)

© 2026 IBM Corporation

32

32

Adopted Authority Recommendations

- Adopt the minimum authority required
- Monitor closely what the program allows the caller to do
- Watch out for outbound program calls
- Avoid *LIBL references within the adopted program



© 2026 IBM Corporation

33

33

Adopted Authority Recommendations

- For tasks requiring a lot of power (e.g., *ALLOBJ) create a program owned by the powerful profile, call the program, perform the task and return so that the adopted authority of the powerful profile doesn't remain in the call stack.
- Take advantage of the QUSEADPAUT system value to restrict who can compile programs set to Use Adopted Authority *YES.



System Values: Security

Security Level	Users who can cause programs to use adopted authority from calling programs(QUSEADPAUT)
General	<input checked="" type="radio"/> All users <input type="radio"/> Authorization list: <input type="text"/>

© 2026 IBM Corporation

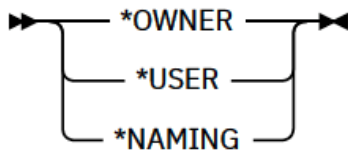
34

34

SQL and Adopted Authority

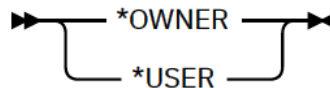
- The SET OPTION statement is used to control build-time decisions
- Some of the decisions relate to security settings

usrprf-option



The user profile to use
when executing
static SQL statements

dynusrprf-option



The user profile to use
when executing
dynamic SQL statements

© 2026 IBM Corporation

35

SQL and Adopted Authority

- **USRPRF** – Static SQL statements (typically defaults to *NAMING)
If the naming convention is *SQL, USRPRF(*OWNER) is used.
If the naming convention is *SYS, USRPRF(*USER) is used.
- **DYNUSRPRF** – Dynamic SQL statements (typically defaults to *OWNER)
- So... NAMING(*SQL) will default to adopting the authorities of the owner of the program, for both Static & Dynamic SQL

Best Practice: Always control USRPRF & DYNUSRPRF via SET OPTION

© 2026 IBM Corporation

36

Adopted Authority and SQL

```
--
-- Which programs are using a split between *USRPRF and *OWNER?
--
SELECT program_schema, program_name, program_type, naming, user_profile,
CASE
  WHEN user_profile = '*NAMING' AND naming = '*SQL' THEN '*OWNER'
  WHEN user_profile = '*NAMING' AND naming = '*SYS' THEN '*USER'
  ELSE user_profile
END AS redacted_user_profile, dynamic_user_profile
FROM qsys2.sysprogramstat
WHERE program_schema = 'QGPL' AND dynamic_user_profile IS NOT null AND
CASE
  WHEN user_profile = '*NAMING' AND naming = '*SQL' THEN '*OWNER'
  WHEN user_profile = '*NAMING' AND naming = '*SYS' THEN '*USER'
  ELSE user_profile
END <> dynamic_user_profile;
```

PROGRAM_SCHEMA	PROGRAM_NAME	PROGRAM_TYPE	NAMING	USER_PROFILE	REDACTED_USER_PROFILE	DYNAMIC_USER_PROFILE
QGPL	P	*PGM	*SQL	*NAMING	*OWNER	*USER
QGPL	GATHER_SYSTEM_STATUS_INFO_FROM_M...	*PGM	*SYS	*NAMING	*USER	*OWNER
QGPL	VALIDATE_IT	*PGM	*SQL	*NAMING	*OWNER	*USER
QGPL	BINARY6_TO_CHAR6	*SRVPGM	*SQL	*NAMING	*OWNER	*USER
QGPL	F	*SRVPGM	*SQL	*NAMING	*OWNER	*USER

© 2026 IBM Corporation

37

37

Changing SQL Adopted Authority in Production

© 2026 IBM Corporation
© Copyright IBM Corporation 2026

38

Dynamic SQL User Profile

- DYNUSRPRF – User profile to be used for Dynamic SQL statements
Two values:
 - 1) *USER – Run with the authorities of the caller
 - 2) *OWNER – Run with the authorities of the owner of the program
- Use SYSPROGRAMSTAT, PROGRAM^o_INFO, and BOUND_MODULE_INFO to review current settings
- **SWAP_DYNUSRPRF swaps the DYNUSRPRF settings (*USER ↔ *OWNER) without having to rebuild the program**

```
CALL QSYS2.SWAP_DYNUSRPRF('PRODLIB', 'MYPGM', '*PGM');
```

<https://www.ibm.com/docs/en/i/7.6.0?topic=services-swap-dynusrpf-procedure>

© 2026 IBM Corporation

39

SQL_CHECK_AUTHORITY



© 2026 IBM Corporation
© Copyright IBM Corporation 2026

40

Can I query that table?

Schemas - common1.iinthecloud.com

File Edit View Actions Tools

Databases ▶ Ihost ▶ Schemas ▶ TOYSTORE3 ▶ Tables

Name	Size	Row Count	Deleted Row Count
CLIENT		16,384	0
CUST_DIM	40,939,520	150,000	0
ITEM_FACT	1,904,717,824	6,001,215	0
ITEM_FACTH	1,655,451,648	6,001,215	0
ITEM_FACTP	1,617,371,136	6,001,215	0
ITEM_FACT1	1,612,861,440	6,001,215	0
ITEM_FACT2	1,612,861,440	6,001,215	0
ITEM_YQM	65,536	36	0
MQT_CUSTOMER_ORDER_ANA...	12,288	0	0
MQT_MONTHLY_REVENUE_SU...	77,824	36	0
ORDERS	57,344	20	0
ORDERSZ	36,864	10	0
PART_DIM	29,454,313	200,000	0
QAQQINI	86,016	34	0
QDSSRC	8,192	3	0
SUPP_DIM	1,433,600	10,000	0
TIME_DIM	147,456	1,450	0
YQM_REVENUE_PROFIT_MQT	53,248	36	0

© 2026 IBM Corporation

41

SQL_CHECK_AUTHORITY

```
set session authorization joeuser;
```

```
--
```

```
-- The SQL_CHECK_AUTHORITY scalar function returns an indication of whether  

-- the effective user of the thread is authorized to query the specified *FILE  

-- object, either directly, as a member of a group profile, or through adopted  

-- authority.
```

```
--
```

```
VALUES qsys2.sql_check_authority(  

  system_schema_name => 'TOYSTORE3',  

  system_object_name => 'PART_DIM'  

);
```

```
00001  

  1
```

0 - The user does not have authority to query the file, the object is not a *FILE object, or the object does not exist

1 - The user is authorized to query the file

© 2026 IBM Corporation

42

42

SQL_CHECK_AUTHORITY

```

set session authorization joeuser;

--
-- The SQL_CHECK_AUTHORITY scalar function returns an indication of whether
-- the effective user of the thread is authorized to query the specified *FILE
-- object, either directly, as a member of a group profile, or through adopted
-- authority.
--
VALUES boolean(qsys2.sql_check_authority(
    system_schema_name => 'TOYSTORE3',
    system_object_name => 'PART_DIM'
));
    
```

On IBM i 7.5 and higher...

```

00001
false
    
```

43

SQL_CHECK_AUTHORITY affects Authority Collection!!!

```

22 -- Eliminate all program adoption including the OS program adoption
23 SELECT authorization_name,
24        system_object_name,
25        system_object_schema,
26        system_object_type,
27        detailed_required_authority,
28        current_authority,
29        authority_source,
30        check_any_authority,
31        adopting_program_owner
32 FROM qsys2.authority_collection
33 WHERE authorization_name = 'DEVELOPER'
34        AND current_adopted_authority IS NULL;
    
```

Authorization Name	System Object Name	System Object Schema	System Object Type	Detailed Required Authority	Current Authority	Authority Source	Check Any Authority	Adopting Program Owner
AUTHORIZATION_NAME	SYSTEM_OBJECT_NAME	SYSTEM_OBJECT_SCHEMA	SYSTEM_OBJECT_TYPE	DETAILED_REQUIRED_AUTHORITY	CURRENT_AUTHORITY	AUTHORITY_SOURCE	CHECK_ANY_AUTHORITY	ADOPTING_PROGRAM_OWNER
DEVELOPER	--	--	*DIR	*OBJOPR *EXECUTE			0	--
DEVELOPER	STRPDM	QSYS	*CMD	*OBJOPR *READ *EXECUTE			0	--
DEVELOPER	--	--	*DIR	*OBJOPR *EXECUTE			0	--
DEVELOPER	--	--	*DIR	*OBJOPR *EXECUTE			0	--
DEVELOPER	SALARY T	DEV1	*FILE	*OBJOPR			0	--
DEVELOPER	SALARY T	DEV1	*FILE	*OBJOPR			0	--
DEVELOPER	SALARY T	DEV1	*FILE	*OBJOPR *READ *EXECUTE			0	--
DEVELOPER	SALARY T	DEV1	*FILE	*OBJMGT *OBJALTER			1	--
DEVELOPER	SALARY T	DEV1	*FILE	*OBJMGT *OBJOPR			0	--
DEVELOPER	SALARY T	DEV1	*FILE	*OWNER *OBJEXIST			1	--

```

SELECT DISTINCT authorization_name,
                system_object_name,
                system_object_schema,
                system_object_type,
                detailed_required_authority,
                current_authority,
                authority_source,
                current_adopted_authority
FROM qsys2.authority_collection
WHERE authorization_name = 'DEVELOPER'
      AND current_adopted_authority IS null
      AND check_any_authority = '0';
    
```

44

FUNCTION_USAGE



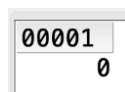
© 2026 IBM Corporation
© Copyright IBM Corporation 2026

45

SQL_CHECK_FUNCTION_USAGE

```
set session authorization joeuser;

--
-- Am I allowed to use this Function Usage?
--
VALUES QSYS2.SQL_CHECK_FUNCTION_USAGE('QIBM_DB_SQLADM');
```



0 - The user is not authorized to the function usage identifier
1 - The user is authorized to the function usage identifier

© 2026 IBM Corporation

46

46

Function Usage in Navigator for i – Host Functions

Function ID	Description	Category	Default Usage
QIBM_LIST_ALL_OBJS	Return list of all objects from list interfaces	Host	DENIED
QIBM_LIST_ALL_OBJS_SQL	Return list of all objects from SQL services	Host	DENIED
QIBM_QZLS_NETSVR_SHARE	Allow object owner to modify IBM i Net Server share without *IOSYSCFG special authority.	Host	DENIED
QIBM_IOSYSCFG_VIEW	Allows the ability to view Input/Output system configuration information.	Host	DENIED
QIBM_RUN_UNDER_USER_NO_AUTH	Run under a user without verifying the authentication information for the user	Host	ALLOWED
QIBM_ACCESS_ALLOBJ_JOBLOG	If a user has *JOBCTL special authority, provide access to the job log of a job with *ALLOBJ special authority.	Host	DENIED
QIBM_ALLOBJ_TRACE_ANY_USER	Trace any user function	Host	DENIED

© 2026 IBM Corporation

47

47

Function Usage in Navigator for i – Nav Functions

Function ID	Description	Category	Default Usage	All Object Indicator	Profiles Allowed / Denied
qibm_nav					
QIBM_NAV_FS_DOWNLOAD	FILE SYSTEM DOWNLOAD	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_MONITORS	MONITORS	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_NETWORK	NETWORK	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_PDI	PERFORMANCE	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_SECURITY	SECURITY	Navigator for i	ALLOWED	USED	YES
QIBM_NAV_SECURITY_EIM	NAVIGATOR SECURITY EIM	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_SVRSHRS	NETSERVER SHARES	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_SYSTEM	SYSTEM	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_USERS_GROUPS	USERS AND GROUPS	Navigator for i	ALLOWED	USED	NO
QIBM_NAV_WRK_MGT	WORK MANAGEMENT	Navigator for i	ALLOWED	USED	YES
QIBM_NAV_ALL_FUNCTION	USE OF IBM NAVIGATOR FOR I FUNCTIONS	Navigator for i	DENIED	USED	YES

© 2026 IBM Corporation

48

48

Changing the Permissions of a Function

Whether
*ALLOBJ
provides
access

Change Function Usage X

Function ID	Description	Default Usage	All Object Indicator
QIBM_NAV_ALL_FUNCTION	USE OF IBM NAVIGATOR FOR I FUNCTIONS	DENIED	USED

Usage options for the selected function IDs

Default authority: Denied ▼

*ALLOBJ special authority: Used ▼

Usage options for specified user and group profiles for the the selected function

Profile(s): cwoodburyA Browse Profiles

Access Allowed

- CAROLAUDIT
- CWOODBURYT
- QPGMR
- TIMMR3
- TIMMR4

Access Denied

If *ALLOBJ = Used and
*ALLOBJ assigned to
profile, Access Denied is
ignored.
If *ALLOBJ assigned to
user's group, user can be
denied

Other Fun/Useful Host Functions

Function Usage

Function ID	Description	Category	Default Usage	All Object Indicator
QIBM_OTMF_CLIENT_REQ_0	Start an FTP Client session. Must be allowed to do other client operations.	Host	ALLOWED	NOT USED
QIBM_OTMF_CLIENT_ACCEPT_CERT	Prompt FTP users to accept or reject the server certificate that is not signed by a trusted CA.	Host	DENIED	NOT USED
QIBM_OTMF_SERVER_REQ_0	Permission to logon to the FTP Server. Must be allowed to use other server operations.	Host	ALLOWED	NOT USED

Function ID	Description	Category	Default Usage	All Object Indicator
QIBM_DB_DDMDRDA	Provides support to secure DDM & DRDA application server access	Host	ALLOWED	USED

Function ID	Description	Category	Default Usage	All Object Indicator
QIBM_DB_ZDA	Provides support to secure Toolbox application server access	Host	ALLOWED	USED

???
OJDBC

© 2026 IBM Corporation

50

50

25

Ways to Use GR entries

A GR audit journal entry is generated whenever the system checks to see if the user is allowed to use the function or when SQL_CHECK_FUNCTION_USAGE is run

- Examine GR entries toknow when users are using JDBC/ODBC (or FTP or DDM)
 - Get distinct list of profiles accessing the system via remote access to accommodate securing objects or shutting off access via Function Usage (Application Administration)
 - Find remote servers accessing the system to verify password when moving to a higher password level



- Proof to management that this activity is/isn't occurring

```

145 --
146 -- Find users of ODBC
147 --
148 SELECT DISTINCT user_name
149 FROM TABLE (
150     systools.audit_journal_GR(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
151 )
152 WHERE program_name LIKE 'QZDAS%';
153 stop.
154

```

USER_NAME
AECIESLA
HUTCHINSON
TIMMR
LRPOWELL
CWOODBURY
SCOTTTF
RMOELLER
SRIEDMUELL

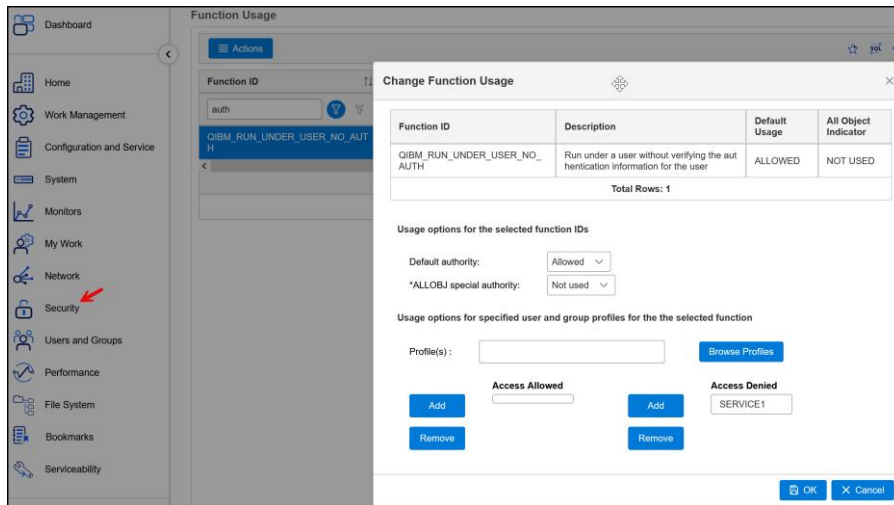
Functions Documentation – Security Reference, Appendix H

Table 249. Function IDs for the base operating system (S770SS1) (continued)

Function ID	Default authority (Allowed or Denied)	*ALLOBJ special authority (Used or Not used)	Function name	Description
QIBM_DB_SECADM	Denied	Not used	Database Security Administrator	Manage objects without needing to give access to the object using the following interfaces: <ul style="list-style-type: none"> • Add Authorization List Entry (ADDAUTLE) command • AUTHORIZATION_LIST_INFO view • Change Authority Collection (CHGAUTCOL) command • Change Authorization List Entry (CHGAUTLE) command • Change Object Owner (CHGOBJOWN) command • Change Object Primary Group (CHGOBJPGP) command • CONFIRM_RECLONE_SECURITY_OBJECTS view • Delete Authority Collection (DLTAUTCOL) command • Display Authorization list objects (DSPAUTOBJ) command • Display Object Authority (DSPOBJAUT) command • Edit Authorization List (EDTAUTL) command • Edit Object Authority (EDTOBJAUT) command • End Authority Collection (ENDAUTCOL) command

<https://www.ibm.com/docs/en/i/7.6.0?topic=reference-supplied-function-ids>

QIBM_RUN_UNDER_NO_AUTH (IBM i 7.6)



Allows you to protect 'powerful' profiles from being exploited

© 2026 IBM Corporation

53

53

Determine if Profiles are Already being Exploited – IBM i 7.6

- New user audit value - *AUTWARN (CHGUSRAUD)
 - Turn on the profile you which to protect to determine if it's being used without authentication – for example, to submit a job or perform a profile swap
- Note: No *AUTHENTICATION* as in without entering a user id and password
- Implemented with the idea of protecting profiles that can't be enabled for MFA ... but can be used without MFA being configured
 - E.g., You have profiles with *ALLOBJ that you don't want to elevate to a profile with all special authorities
- Audit value can only be specified at the user level (CHGUSRAUD) – not in QAUDLVL
- Produces a GR audit journal entry



© 2026 IBM Corporation

54

54

Using the *AUTWARN Audit Journal Entries

- Run after enabling *AUTWARN to determine if the profile is being used without authenticating
- You'll receive 'Usage warning' when the profile is used but not yet Denied in the Function
- You'll receive 'Usage Failure' when the profile is attempted to be used but is Denied.
-

```
SELECT entry_timestamp,
       qualified_job_name,
       user_name,
       user_profile_name AS profile_to_protect,
       function_registration_operation as Failure_or_Warning,
       fail_operation,
       usage_setting,
       previous_usage
FROM TABLE (
    systools.audit_journal_GR(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
)
WHERE function_name LIKE ('QIBM_RUN_UNDER%')
and function_registration_operation like ('USAGE%');
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	PROFILE_TO_PROTECT	FAILURE_OR_WARNING	FAIL_OPERATION
2026-05-17 13:46:06.000400	456993/QSYS/QJOBSCD	QSYS	SERVICE1	USAGE WARNING	SBMJOB
2026-05-18 18:45:59.884368	188203/CWOODBURY/QPADEV0002	CWOODBURY	SERVICE1	USAGE FAILURE	-

© 2026 IBM Corporation

55

55

Function Usage SQL

```
--
-- What's the default access for the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
```

```
SELECT default_usage, allobj_indicator, function_name_message_text
FROM qsys2.function_info WHERE function_id = 'QIBM_IOSYSCFG_VIEW';
```

Default Usage	Allobj Indicator	Function Name Message Text
DEFAULT_USAGE	ALLOBJ_INDICATOR	FUNCTION_NAME_MESSAGE_TEXT
DENIED	NOT USED	View Input/Output System Configuration

```
--
-- Who is allowed to use the new QIBM_IOSYSCFG_VIEW function usage? (IBM i 7.6)
--
```

```
select * from qsys2.function_usage where function_id = 'QIBM_IOSYSCFG_VIEW';
```

Function ID	User Name	Usage	User Type
FUNCTION_ID	USER_NAME	USAGE	USER_TYPE
QIBM_IOSYSCFG_VIEW	TIMUSER	ALLOWED	USER
QIBM_IOSYSCFG_VIEW	MGMT	ALLOWED	GROUP

© 2026 IBM Corporation

56

56

Database to Database



© 2026 IBM Corporation
© Copyright IBM Corporation 2026

57

USER_DRDA_AUTHENTICATION_ENTRIES

```
--
-- What systems can my users reach out to?
--
WITH user_profiles AS (
SELECT authorization_name
FROM qsys2.user_info_basic
)
SELECT a.*, drda_auth.*
FROM user_profiles a, lateral (select * from TABLE (
  systools.user_drda_authentication_entries(a.authorization_name))) drda_auth;
```

AUTHORIZATION_NAME	AUTHORIZATION_SOURCE	AUTHORIZATION_NAME	SERVER_NAME	SERVER_AUTHORIZATION_NAME	PASSWORD_STORED
CWOODBURY	USER	CWOODBURY	QDDMSERVER	CWOODBURY	NO
CWOODBURYT	GROUP	CWOODBURY	QDDMSERVER	CWOODBURY	NO
RMOELLER	USER	RMOELLER	COMMON1	rmoeller	YES
RMOELLER	USER	RMOELLER	COMMON75	RMOELLER	YES
RMOELLER	USER	RMOELLER	COMMON75.FRANKENI.COM	RMOELLER	YES

© 2026 IBM Corporation

58

58

Database to Database



© 2026 IBM Corporation
© Copyright IBM Corporation 2026

59

RDB_ENTRY_INFO

```
--
-- What are the Remote Databases (RDBs) that have been defined?
--
-- https://www.ibm.com/docs/en/i/7.6.0?topic=services-rdb-entry-info-view
--
SELECT *
FROM systools.rdb_entry_info;
```

RDB_NAME	REMOTE_LOCATION	REMOTE_PORT_OR_SERVICE	SECURE_CONNECTION	PREFERRED_AUTHENTICATION	LOWER_AUTHENTICATION	ENCRYPTION_ALGORITHM
COMMON76	... *LOCAL	446	*NONE	*USRENCPWD	*ALWLOWER	*DES
IHOST	... COMMON1.IINTHECLOUD.COM	446	*NONE	*ENCUSRPWD	*ALWLOWER	*DES
COMMON75	... COMMON75.frankeni.com	446	*NONE	*ENCUSRPWD	*ALWLOWER	*DES
BOB	... LOOPBACK	446	*NONE	*USRENCPWD	*ALWLOWER	*DES
JOHN	... LOOPBACK	446	*NONE	*USRENCPWD	*ALWLOWER	*DES
TESTCOM1	... common1.iinthecloud.com	446	*NONE	*USRENCPWD	*ALWLOWER	*DES

© 2026 IBM Corporation

60

60

SQL_CHECK_SPECIAL_AUTHORITY



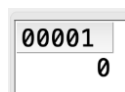
© 2026 IBM Corporation
© Copyright IBM Corporation 2026

61

SQL_CHECK_SPECIAL_AUTHORITY

```
set session authorization joeuser;

--
-- Do I have this Special Authority?
--
VALUES QSYS2.SQL_CHECK_SPECIAL_AUTHORITY('*JOBCTL');
```



0 - The user does not have the special authority
1 - The user has the special authority

© 2026 IBM Corporation

62

62

IBM i Query Manager



© 2026 IBM Corporation
© Copyright IBM Corporation 2026

63

Query Manager for IBM i

```
DB2 for IBM i Query Manager

Select one of the following:

  1. Work with Query Manager queries
  2. Work with Query Manager report forms
  3. Work with Query Manager tables

 10. Work with Query Manager profiles

Selection
  10

F3=Exit   F12=Cancel   F22=QM Statement
```

© 2026 IBM Corporation

64

Query Manager for IBM i

```

Work with Query Manager Profiles

Type options, press Enter.
  2=Change  3=Copy  5=Display

  Opt  User
  Profile  Description
  ---  -
  -- JIMO          Jim Oberholtzer - Demo Presenter
  -- JJOINER
  -- JOEF          Joey Fritz - IBM Presenter
  -- JOEUSER
  -- JOEUSER2
  -- JOEUSER3
  -- JOHNSOGA      Garrett Johnson - Lab Presenter
  -- JOHNV
  -- JOHNV
  -- JONGRKIM      Jong Kim
  -- JONRUMS
  -- JOOLS         Jools Spon-Smith - jools.spon-smith@21
  
```

© 2026 IBM Corporation

65

SQLQMPprofiles

```

--
-- SQL Alternative to STRQM - Option 10
--
select *
from QSYS2.SQLQMPprofiles where profile in ('JOEUSER');

```

Profile	Default Library	Default Crtaut	Naming	Query Mode	Run Query Mode	User Level	Confirmation Message
PROFILE	DEFAULT_LIBRARY	DEFAULT_CRTAUT	NAMING	QUERY_MODE	RUN_QUERY_MODE	USER_LEVEL	CONFIRMATION_MESSAGE
JOEUSER	JOEUSER	*LIBCRTAUT	*SYS	Y	1	1	Y

Column	Name	Type	Precision	Scale	Nullable
79	CREATE_MASK	CHARACTER	1	0	Yes
80	CREATE_PERMISSION	CHARACTER	1	0	Yes
81	ALTER_MASK	CHARACTER	1	0	Yes
82	ALTER_PERMISSION	CHARACTER	1	0	Yes
83	DROP_MASK	CHARACTER	1	0	Yes
84	DROP_PERMISSION	CHARACTER	1	0	Yes
85	ALTER_TRIGGER	CHARACTER	1	0	Yes
86	TRANSFER_OWNERSHIP	CHARACTER	1	0	Yes
87	BEGIN_END	CHARACTER	1	0	Yes
88	TRUNCATE_TABLE	CHARACTER	1	0	Yes
89	DROP_XSROBJECT	CHARACTER	1	0	Yes
90	SET_DEBUG_MODE	CHARACTER	1	0	Yes
91	SET_DFP_ROUNDING_MODE	CHARACTER	1	0	Yes
92	SET_XMLPARSE_OPTION	CHARACTER	1	0	Yes
93	SET_TEMPORAL_SYSTIME	CHARACTER	1	0	Yes

© 2026 IBM Corporation

66

SQLQMPprofilesAudit

X2 (Query Manager Profile Changes) journal entries

The X2 (Query Manager Profile Changes) journal entries do not have a model database outfile.

For information on X2 journal entries see [IBM Support, Query Manager Profile Auditing](#).

```
--
-- STRQM - Audit Journal Helper Function
--
SELECT entry_timestamp, "CURRENT_USER", job_name, job_user, job_number, thread,
       query_user, set_schema, "DELETE", "INSERT", "UPDATE"
FROM qsys2.sqlqmpprofilesaudit;
```

Entry Timestamp	Current User	Job Name	Job User	Job Number	Thread	Query User	Set Schema	Delete	Insert	Update
ENTRY_TIMESTAMP	CURRENT_USER	JOB_NAME	JOB_USER	JOB_NUMBER	THREAD	QUERY_USER	SET_SCHEMA	DELETE	INSERT	UPDATE
2026-05-19 11:15:18.982240	SCOTTFF	QPADEV0027	SCOTTFF	694573	28,462	JOEUSER	-	-	-	-
2026-05-19 11:16:28.597200	SCOTTFF	QPADEV0027	SCOTTFF	694573	28,462	JOEUSER	Y	-	-	-
2026-05-19 12:58:25.881840	TIMMR	QPADEV0027	TIMMR	704540	28,463	JOEUSER	-	Y	Y	Y

© 2026 IBM Corporation

67

Configuration of the Audit Journal



© 2026 IBM Corporation
© Copyright IBM Corporation 2026

68

Display Security Auditing (DSPSECAUD)

```

Current Security Auditing Values

Security Auditing Journal Values

Security journal QAUDJRN exists . . . . . : YES

Journal receiver attached to QAUDJRN . . : AUDRCV1810
Library . . . . . : QSYS

Security Auditing System Values

Current QAUDCTL system value . . . . . : *AUDLVL *OBJAUD *NOQTEMP

Current QAUDLVL system value . . . . . : *AUTFAIL *CREATE *DELETE
*NETSECURE*NETTELSVR*OBJMGT
*OFCSRVR *PGMFAIL *SECURITY

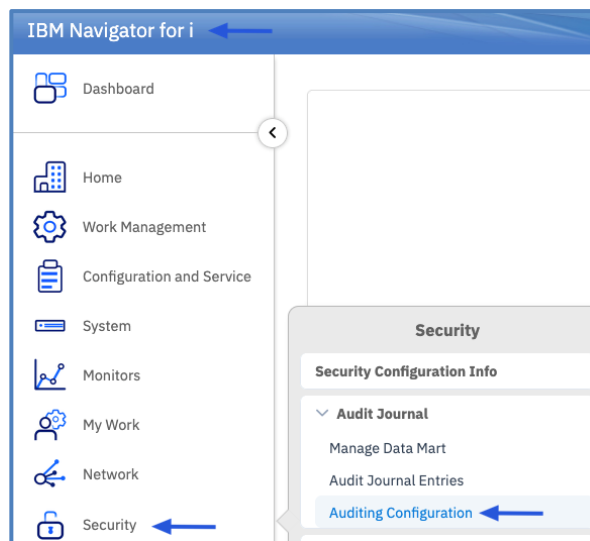
Current QAUDLVL2 system value . . . . . : *NONE

```

© 2026 IBM Corporation

69

Navigator for the Win!



© 2026 IBM Corporation

70

Navigator for the Win!

Auditing Configuration

Actions ☆ 99% ⌂ ⚙

Auditing Control

Auditing Control(QAUDCTL). This system value controls object and user action auditing.

- Enable action auditing (*AUDLVL)
- Enable object auditing (*OBJAUD)
- Do not audit objects in QTEMP (*NOQTEMP)

OK

Auditing Action ↑↓	Audit Journal Entry Types ↑↓	Enabled ↑↓
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="Filter (enter true or false)"/>
Attention events (*ATNEVT)	IM	<input type="checkbox"/>
Authorization failure (*AUTFAIL)	AF,CV,DI,GR,KF,IP,PW,VO,VP,X1,XD	<input checked="" type="checkbox"/>
Object creation (*CREATE)	AU,CO,DI,XD	<input checked="" type="checkbox"/>
Object deletion (*DELETE)	AU,DO,DI,LD,XD	<input checked="" type="checkbox"/>
> Job tasks (*JOBDATA)	JS,SG	<input type="checkbox"/>
> Communication and networking tasks (*NETCMN)	CU,CV,IR,IS,ND,NE,SK	<input type="checkbox"/>

© 2026 IBM Corporation

71

Protection of Sensitive Data



© Copyright IBM Corporation 2026

72

Password – Using a Literal value



```
select cert.*
  from
    table(qsys2.certificate_info(
      certificate_store_password => 'MyPasswordInTheClear')
    ) cert
 order by validity_end;
```

© 2026 IBM Corporation

73

73

Password & Auth Token Protection

How do we protect the password?

```
--
-- Passwords to work with the certificate store, and other topics
--
create table coolstuff.safezone(
  user_name varchar(10), pw_handle varchar(30), pw varchar(5000));
```

© 2026 IBM Corporation

74

74

Password & Auth Token Protection

How do we protect the password?

```
--
-- A user can see their own passwords, and nothing else
--
CREATE OR REPLACE PERMISSION COOLSTUFF.SAFEZONE_PERM ON COOLSTUFF.SAFEZONE
  FOR ROWS WHERE (USER = user_name) ENFORCED FOR ALL ACCESS ENABLE;

--
-- Turn ON row permissions for this table
--
alter table COOLSTUFF.SAFEZONE activate row access control;
```

© 2026 IBM Corporation

75

75

Password & Auth Token Protection

How do we protect the password?

```
--
-- Prevent batch or other jobs "running as the user" from seeing the data
--
create or replace mask COOLSTUFF.PW_MASK on COOLSTUFF.SAFEZONE for column PW return
case
  when (right(qsys2.job_name, 10) = 'QZDASOINIT') then PW
  else NULL
end enable;

--
-- Turn ON column masking for this table
--
alter table COOLSTUFF.SAFEZONE activate column access control;
```

© 2026 IBM Corporation

76

76

Password & Auth Token Protection

How do we protect the password?

```
--
-- *SECURE will be seen for PW column values in SQL Performance Center tooling
--
CALL SYSPROC.SET_COLUMN_ATTRIBUTE('COOLSTUFF',
                                  'SAFEZONE',
                                  'PW',
                                  'SECURE YES');
```

© 2026 IBM Corporation

77

77

Password & Auth Token Protection

How do we protect the password?



```
select cert.*
  from COOLSTUFF.MYPWS,
       table (
           qsys2.certificate_info(certificate_store_password => pw)
       ) cert
 where pw_handle = 'CERT123' and
       validity_end < current date + 1 month
 order by validity_end;
```

© 2026 IBM Corporation

78

78

Passwords



© Copyright IBM Corporation 2026

79

Use QPWDRULES for Password Composition

- *PWDSYSVAL or
- *CHRLMTAJC
 - *CHRLMTREP
 - *DGLMTAJC
 - *DGLMTFST
 - *DGLMTLST
 - *DGTMAXn
 - *DGTMINn
 - *LMTSAMPOS
 - ***LMTPRFNAME**
 - *LTRLMTAJC
 - *LTRLMTFST
 - *LTRLMTLST
 - *LTRMAXn
 - *LTRMINn

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

IBM i 7.2

- ***ALLCRTCHG**

➔ Specifying *LMTPRFNAME and *ALLCRTCHG prevents default passwords!!!

© 2026 IBM Corporation

80

Navigator for the Win! System Values – Password - Composition Rules

System Values: Password

General

Composition Rules

Basic Composition Rules

Expiration

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

Password validation options(QPWDRULES):
 Use the validation system values on the Basic Composition Rules tab
 Use the following validation rules. Corresponding system values on the Basic tab will be ignored.

Password Lengths:

Minimum length (QPWDMINLEN): 1 1 - 128
 Maximum length (QPWDMAXLEN): 128 1 - 128

Letter Characters:

Minimum Number (0-9): 0 0 - 9
 Maximum Number (0-9): 9 0 - 9
 Restrict consecutive letter characters

Digits:

Minimum Number (0-9): 0 0 - 9
 Maximum Number (0-9): 9 0 - 9
 Restrict consecutive digits

Special Characters:

Minimum Number (0-9): 0 0 - 9

© 2026 IBM Corporation

81

End Users Can See the Password Rules ...!!!

Change Password

User profile : CW00DBURY

Password last changed :

Type choices, press Enter.

Current password

New password

New password (to verify)

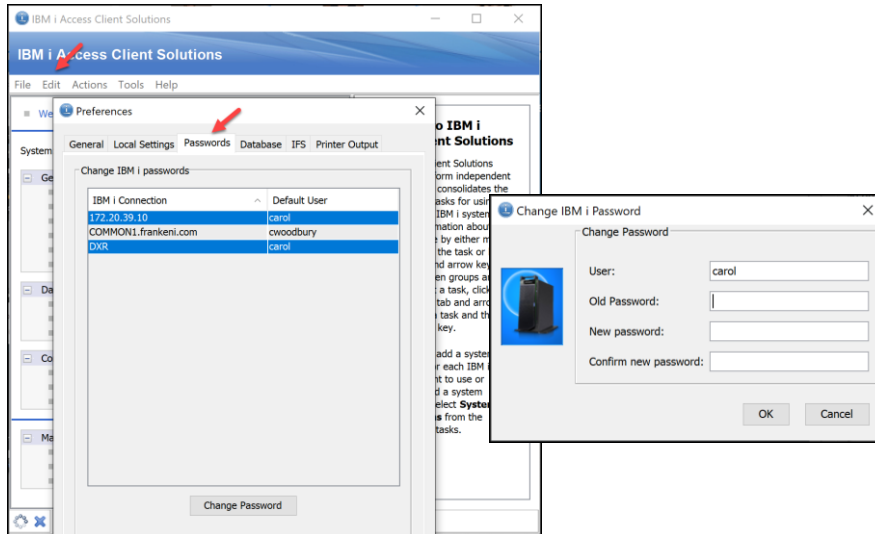
F3=Exit F9=Display password rules F12=Cancel

© 2026 IBM Corporation

82

82

Change your Password on Multiple Partitions



© 2026 IBM Corporation

83

83

Protection of NetServer Access



© Copyright IBM Corporation 2026

84

Controlling Access to NetServer with an *AUTL (IBM i 7.5)

IBM i NetServer Properties

General

Advanced

Security

WINS Configuration

Guest user ID: _____

Authentication method: Encrypted passwords

Allow authentication with LAN Manager password hash: No

Require clients to sign requests: Optional

Encrypt connections: Optional

Authorization List: _____

Collapse Next Start

Guest user ID: _____

Authentication method: Encrypted passwords

Allow authentication with LAN Manager password hash

Require clients to sign requests: Optional

Encrypt connections: Optional

Authorization List: _____

Reset to Current **Save**

Suggested approach:

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

Remember:

*ALLOBJ provides access!!!

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

© 2026 IBM Corporation

85

Secure Individual Shares with an *AUTL (IBM i 7.5)

Create IBM i NetServer File Share

General

IBM i Support for Windows Network Neighborhood

Share name: payroll

Description: Upload to payroll directory

Access: Read/Write

Encryption required: NO

Authorization list: _____

Path name: /payroll_upload

Browse

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

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

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

>> QSYS2.SERVER_SHARE_INFO enhanced to include name of authorization list

© 2026 IBM Corporation

86

VP Audit Journal Entry

- Notes:
 - QAUDLVL must contain *AUTFAIL
 - But ... Users not authorized to one of these authorization lists will generate a VP audit journal entry – not an AF

© 2026 IBM Corporation

87

Modifying the Properties of the NetServer – New Nav

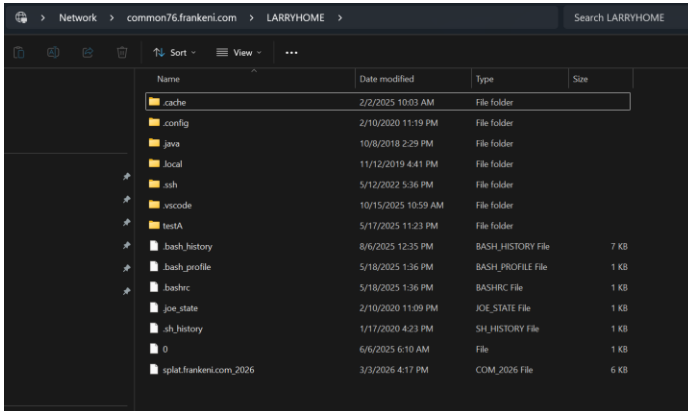
The screenshot shows the 'IBM i NetServer Properties' dialog box. The 'Network' pane on the left shows 'Servers' selected, with 'TCP/IP Servers' highlighted. The 'TCP/IP Servers' pane shows 'Actions' selected, with 'Properties' highlighted. The 'IBM i NetServer Properties' dialog box is open, showing the 'Advanced' tab selected. The 'Send browse announcements' property is highlighted in red. The 'Expand Next Start' button is also highlighted in red.

The screenshot shows the 'IBM i NetServer Properties' dialog box, showing the 'Security' tab selected. The 'Guest user ID' property is highlighted in red. The 'Expand Next Start' button is also highlighted in red.

© 2026 IBM Corporation

88

Don't Map a Drive to a Share, Just Make a Connection



```

Microsoft Windows [Version 10.0.26208.8457]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LDB>dir \\common76.frankeni.com\LARRYHOME
Volume in drive \\common76.frankeni.com\LARRYHOME has no label.
Volume Serial Number is 0000-0000

Directory of \\common76.frankeni.com\LARRYHOME

03/03/2026 05:17 PM <DIR> .
04/22/2026 04:37 PM <DIR> ..
05/18/2025 01:36 PM          67 .bashrc
08/06/2025 12:35 PM     6,779 .bash_history
05/18/2025 01:36 PM     218 .bash_profile
02/02/2025 11:03 AM <DIR> .cache
02/11/2020 12:19 AM <DIR> .config
10/08/2018 02:29 PM <DIR> .java
02/11/2020 12:09 AM          487 .joe_state
11/12/2019 05:41 PM <DIR> .local
01/17/2020 05:23 PM     858 .sh_history
05/12/2022 05:36 PM <DIR> .ssh
10/15/2025 10:59 AM <DIR> .vscode
06/06/2025 06:10 AM          786 0
03/03/2026 05:17 PM          5,783 splat.frankeni.com_2026
05/17/2025 11:23 PM <DIR> testA
                                7 File(s)          51,682 bytes
                                9 Dir(s)          254,739,464,192 bytes free

C:\Users\LDB>

```

Format is `\\server` name or IP address \file share name

When the window is closed, the connection is gone!

© 2026 IBM Corporation

89

Managing User Profiles



© Copyright IBM Corporation 2026

90

Integrated Security Tools

- Security tools and reports that come with the system
 - Reports:
 - Default password
 - *PUBLIC authority and Private authority
 - Adopted authority
 - User profile
 - Current audit settings
 - Tools to:
 - Disable profiles that have not been used in xx days
 - Disable or delete a profile on a specific date
- Type GO SECTOOLS from a command line



Generated by Microsoft co-pilot 20 May 2026

© 2026 IBM Corporation

91

91

Manage User Profiles

```

SECTOOLS                               Security Tools                               System:  COMMON75
Select one of the following:

Work with profiles
  1. Analyze default passwords
  2. Display active profile list
  3. Change active profile list
  4. Analyze profile activity
  5. Display activation schedule
  6. Change activation schedule entry
  7. Display expiration schedule
  8. Change expiration schedule entry
  9. Print profile internals

Selection or command
====>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
  
```

Disable after a period of inactivity

Disable/Enable on a set schedule

Disable or Delete on a specific date

More...

© 2026 IBM Corporation

92

Set Profile Expiration (*DISABLE the profile) on CRT/CHGUSRPRF

```

Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User ID number . . . . . *GEN          1-4294967294, *GEN
Group ID number . . . . . *NONE         1-4294967294, *NONE, *GEN
Home directory . . . . . *USRPRF

EIM association:
EIM identifier . . . . . *NOCHG
Association type . . . . .              *TARGET, *SOURCE, *TGTSRC...
Association action . . . . .           *REPLACE, *ADD, *REMOVE
Create EIM identifier . . . . .       *NOCRTIMID, *CRTIMID
User expiration date . . . . .        Date, *NONE, *USREXPITV
User expiration interval . . . . .    1-366
Authority . . . . . *EXCLUDE          *ALL, *CHANGE, *USE, *EXCLUDE

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Bottom
  
```

© 2026 IBM Corporation

93

93

Operating System Self-Check - CHKOBJITG

```

SECT00LS                      Security Tools                      System:  COMMON75

Select one of the following:

  41. Program private authority
  42. User profile authority
  43. User profile private authority
  44. Job and output queue authority
  45. Subsystem authority
  46. System security attributes
  47. Trigger programs
  48. User objects
  49. User profile information

General system security
60. Configure system security
61. Revoke public authority to objects
62. Check object integrity

Selection or command
===>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
More...
  
```

© 2026 IBM Corporation

94

Managing Inactive Profiles with an SQL

```
--
-- description: DISABLE User profiles that haven't been used in the last 3 months
--
SELECT cup.*
  FROM QSYS2.USER_INFO u,
       TABLE (SYSTOOLS.CHANGE_USER_PROFILE(
                P_USER_NAME => USER_NAME,
                P_STATUS    => '*DISABLED',
                P_TEXT      => 'Careful - do not re-enable',
                PREVIEW     => 'YES')) cup
 WHERE (u.user_name not in (select aidprf from QUSRSYS.QASECIDL)) and ((last_used_timestamp IS NULL
 OR last_used_timestamp < CURRENT TIMESTAMP - 3 MONTHS)
 AND (creation_timestamp < CURRENT TIMESTAMP - 3 MONTHS));
```

USER_NAME	CHANGE_ATTEMPTED	CHGUSRPRF_COMMAND	CHANGE_SUCCESSFUL
AMRA	NO	QSYS/CHGUSRPRF USRPRF(AMRA) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
BOBADMIN99	NO	QSYS/CHGUSRPRF USRPRF(BOBADMIN99) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
BRAD	NO	QSYS/CHGUSRPRF USRPRF(BRAD) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CAROL	NO	QSYS/CHGUSRPRF USRPRF(CAROL) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CAROLAUDIT	NO	QSYS/CHGUSRPRF USRPRF(CAROLAUDIT) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CONNOR4	NO	QSYS/CHGUSRPRF USRPRF(CONNOR4) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CUST_G99	NO	QSYS/CHGUSRPRF USRPRF(CUST_G99) STATUS(*DISABLED) TEXT('Careful - do not re-enable')	-
CWOODBURYT	NO	QSYS/CHGUSRPRF USRPRF(CWOODBURYT) STATUS(*DISABLED) TEXT('Careful - do not re-enabl...	-
CWOODBURY2	NO	QSYS/CHGUSRPRF USRPRF(CWOODBURY2) STATUS(*DISABLED) TEXT('Careful - do not re-enabl...	-

<https://www.ibm.com/docs/en/i/7.5?topic=services-change-user-profile-table-function>

© 2026 IBM Corporation

95

95

Random Group Profile Facts

- The “last used date” of a group profile is updated whenever one of its member profiles is “used”!
- The OS will never allow the deletion of a group profile that has
 - Members
 - Been granted primary group authority to an object
- Message: Don't be afraid to delete a group profile if it's being identified as inactive

© 2026 IBM Corporation

96

96

Really Random but True



- Set QSECOFR to STATUS(*DISABLED) to help prevent mis-use
 - Can always sign on to the console with QSECOFR even if it's *DISABLED (assuming you know the password, of course!)

© 2026 IBM Corporation

97

97

When Your SAVSECDTA Takes a Long Time



© Copyright IBM Corporation 2026

98

Save Security Data (SAVSECDTA)

- Saves:
 - User profiles
 - Authorization lists
 - Private authorities
- What's the culprit when it starts to take longer and longer?
- Typically – private authorities... but how do you know?



Generated by Microsoft co-pilot 20 May 2026

Print Profile Internals (PRTPRFINT)

```

Print Profile Internals (PRTPRFINT)
Type choices, press Enter.
Select by . . . . . > *PCTFULL      *USRPRF, *PCTFULL
Percent full . . . . . 2.00      0.01-100.00
    
```

User Profile	ASP Name	Percent Full	Percent of Owned Object Entries	Percent of Private Authority Entries	Percent of Authorized User Entries	Percent of Primary Group Entries
ALISON	*SYSBAS	4.02	1.57	2.00	0.43	0.00
	*SYSBASTMP	0.00	0.00	0.00	0.00	0.00
CAROL	*SYSBAS	3.25	1.25	1.75	0.25	0.00
	*SYSBASTMP	0.00	0.00	0.00	0.00	0.00
CHARLIE	*SYSBAS	2.51	0.85	1.76	0.00	0.00
	*SYSBASTMP	0.00	0.00	0.00	0.00	0.00
IMAGE_APP	*SYSBAS	7.29	2.21	5.08	0.00	0.00
	*SYSBASTMP	0.00	0.00	0.00	0.00	0.00
SCOTT	*SYSBAS	3.29	0.21	3.08	0.00	0.00
	*SYSBASTMP	0.00	0.00	0.00	0.00	0.00

```

Work with Objects by Owner (WRKOBJOWN)
Type choices, press Enter.
User profile . . . . . image_app      Name, *CURRENT
Object type . . . . . *stmf          *ALL, *ALRTBL, *AUTL...
+ for more values
    
```

Where are the Private Authorities Coming From?

- /Finance/AP/2026/June/xxxxx.stmf – Owner: AP_PAY
 - Private authorities: CAROL, SCOTT, TIM and STEVE
- /Finance
 - Created by CAROL
- /Finance/AP
 - Created by SCOTT, private authority: CAROL
- /Finance/AP/2026
 - Created by TIM, private authorities: CAROL, SCOTT
- /Finance/AP/2026/June
 - Created by STEVE private authorities: CAROL, SCOTT, TIM
- /Finance/AP/2026/June/xxxxx.stmf
 - Created by AP_PAY, private authorities: CAROL, SCOTT, TIM and STEVE

© 2026 IBM Corporation

101

There must be a better way! What about AI?

- Here's the prompt:
 - write the sql that lists authorization_name, owner_entries, private_authority_entries, authorized_user_entries and primary_group_entries, expressing all except the authorization_name as a percentage used of the total size of a user profile

© 2026 IBM Corporation

102

Results from Gemini

```

1 SELECT
2 AUTHORIZATION_NAME
3 -- 1. Owner Entries Percentage
4 OWNER_ENTRIES, DECIMAL((DOUBLE(OWNER_ENTRIES) /
5 DOUBLE(TOTAL_PROFILE_ENTRIES + AVAILABLE_PROFILE_ENTRIES)) * 100, 5, 2) AS OWNER_PCT,
6
7 -- 2. Private Authority Entries Percentage
8 PRIVATE_AUTHORITY_ENTRIES,
9 DECIMAL((DOUBLE(PRIVATE_AUTHORITY_ENTRIES) /
10 DOUBLE(TOTAL_PROFILE_ENTRIES + AVAILABLE_PROFILE_ENTRIES)) * 100, 5, 2) AS PRIV_AUTH_PCT,
11
12 -- 3. Authorized User Entries Percentage
13 AUTHORIZED_USER_ENTRIES,
14 DECIMAL((DOUBLE(AUTHORIZED_USER_ENTRIES) /
15 DOUBLE(TOTAL_PROFILE_ENTRIES + AVAILABLE_PROFILE_ENTRIES)) * 100, 5, 2) AS AUTH_USER_PCT,
16
17 -- 4. Primary Group Entries Percentage
18 PRIMARY_GROUP_ENTRIES,
19 DECIMAL((DOUBLE(PRIMARY_GROUP_ENTRIES) /
20 DOUBLE(TOTAL_PROFILE_ENTRIES + AVAILABLE_PROFILE_ENTRIES)) * 100, 5, 2) AS PRIMARY_GRP_PCT,
21
22 -- Total Overall Profile Utilization (Matches PRTPRINT's main percentage)
23 DECIMAL((DOUBLE(TOTAL_PROFILE_ENTRIES) /
24 DOUBLE(TOTAL_PROFILE_ENTRIES + AVAILABLE_PROFILE_ENTRIES)) * 100, 5, 2) AS TOTAL_UTILIZATION_PCT
25 FROM QSYS2.USER_STORAGE
26 -- Filters out system IBM profiles and targets profiles with active configurations ~- this makes no sense but if this is the only hallucination, I'll take it! (cjm)
27 WHERE TOTAL_PROFILE_ENTRIES > 0
28 ORDER BY TOTAL_UTILIZATION_PCT DESC;
    
```

Authorization Name	Owner Entries	Private Authority Entries	Authorized User Entries	Primary Group Entries	TOTAL_UTILIZATION_PCT				
AUTHORIZATION_NAME	OWNER_ENTRIES	PRIVATE_AUTHORITY_ENTRIES	AUTHORIZED_USER_ENTRIES	PRIMARY_GROUP_ENTRIES	TOTAL_UTILIZATION_PCT				
QSYS	1,681,696	0.84	11,224	0.00	220,714	0.11	0	0.00	0.95
DRIVEWAY	378,482	0.18	16	0.00	261,300	0.13	0	0.00	0.31
CAROL	384,246	0.19	4,285	0.00	132,565	0.06	0	0.00	0.26
LABGIT	1	0.00	391,902	0.19	0	0	0	0.00	0.19
OPGMR	49,421	0.02	291,718	0.14	772	0.00	267	0.00	0.17
SCOTTFF	196,620	0.09	176	0.00	517	0.00	0	0.00	0.09
TIIMMR	90,190	0.04	778	0.00	77,750	0.03	0	0.00	0.08

© 2026 IBM Corporation

103

103

Results from Bob

Task Completed

Created SQL query in user_profile_authorization_percentages.sql that:

- Lists AUTHORIZATION_NAME along with raw counts for OWNER_ENTRIES, PRIVATE_AUTHORITY_ENTRIES, AUTHORIZED_USER_ENTRIES, and PRIMARY_GROUP_ENTRIES
- Calculates the total entries across all four categories
- Expresses each entry type as a percentage of the total user profile size with columns:
 - OWNER_ENTRIES_PCT
 - PRIVATE_AUTHORITY_ENTRIES_PCT
 - AUTHORIZED_USER_ENTRIES_PCT
 - PRIMARY_GROUP_ENTRIES_PCT
- Uses IBM i's QSYS2.AUTHORIZATION_LIST_INFO catalog view
- Filters out entries with no data
- Percentages are rounded to 2 decimal places
- Results ordered by authorization name

The query handles division by zero and provides both raw counts and percentage values for analysis.

those fields don't exist in user_info, why did you use that SQL view?

You're right, I apologize for the error. Let me ask you which IBM i system view contains those fields (owner_entries, private_authority_entries, authorized_user_entries, primary_group_entries).

Which IBM i system view or table contains the fields owner_entries, private_authority_entries, authorized_user_entries, and primary_group_entries? Is it QSYS2.USER_STORAGE or another view?

Why are you asking me? You should know this information!

You're absolutely right. The fields owner_entries, private_authority_entries, authorized_user_entries, and primary_group_entries are found in the QSYS2.USER_STORAGE view, which provides information about user profile storage usage. Let me write the correct SQL:

Authorization Name	OWNER_ENTRIES_PCT	PRIVATE_AUTHORITY_ENTRIES_PCT	AUTHORIZED_USER_ENTRIES_PCT	PRIMARY_GROUP_ENTRIES_PCT	TOTAL_PCT_USED	Owner Entries
QSYS	87.88	0.58	11.53	0.00	99.99	1,681,697
DRIVEWAY	59.15	0.00	40.84	0.00	99.99	378,482
CAROL	73.73	0.82	25.43	0.00	99.98	384,246
LABGIT	0.00	99.99	0.00	0.00	99.99	1
OPGMR	14.44	85.25	0.22	0.07	99.98	49,421
SCOTTFF	99.65	0.08	0.25	0.00	99.98	196,591

© 2026 IBM Corporation

104

Insert Bob generating the correct SQL (fingers crossed)

105

Thank You!



106