Security for the modern era of IBM i

Team of IBM Champions and Experts

Carol Woodbury
IBM i Security SME
CISSP, CRISC
IBM CHAMPION

Steve Riedmueller
Director of Security Services
COMMON N2i Chair
IBM CHAMPION

Justin Loeber
Owner & CEO
COMMON Director
IBM i ISV Council

Richard Loeber
Head of Product
Company Founder
Professor Emeritus

kisco

www.kisco.com
sales@kisco.com

7 IBM i Security Tasks for 2025

Justin Loeber
justin@kisco.com

Steve Riedmueller
steve@kisco.com

© Kisco Systems LLC, All Rights Reserved.

Let’s Face it …

Security is *NOT* convenient
Ongoing and time consuming

More Modern
More Efficient
MORE FUN !!!

Task List

- ❑ 1. Assess System Values
- ❑ 2. Perform a User Profile Checkup
- ❑ 3. Protect Your Data
- ❑ 4. Analyze the Audit Journal
- ❑ 5. Review Function Usage Configuration
- ❑ 6. Evaluate File Shares (Netserver)
- ❑ 7. Get/Stay Current
- ❑ 8. BONUS TASK?

kisco

Assess System Values

Assess System Values

- Ensure your current settings meet security best practices:
  - IBM i Security Reference: https://www.ibm.com/docs/en/i/7.5?topic=security-reference
  - IBM i Security Administration and Compliance, 3rd edition by Carol Woodbury
  - https://www.cisecurity.org/benchmark/ibm
  - Risk Assessment output
- Where they don't meet best practices, evaluate the risk:
  - of changing the setting.
  - of not changing the setting.
- Key system values:
  - QSECURITY
  - QPWD*
  - QMAXSIGN
  - QAUD*
  - QCRTAUT
  - QSSL*

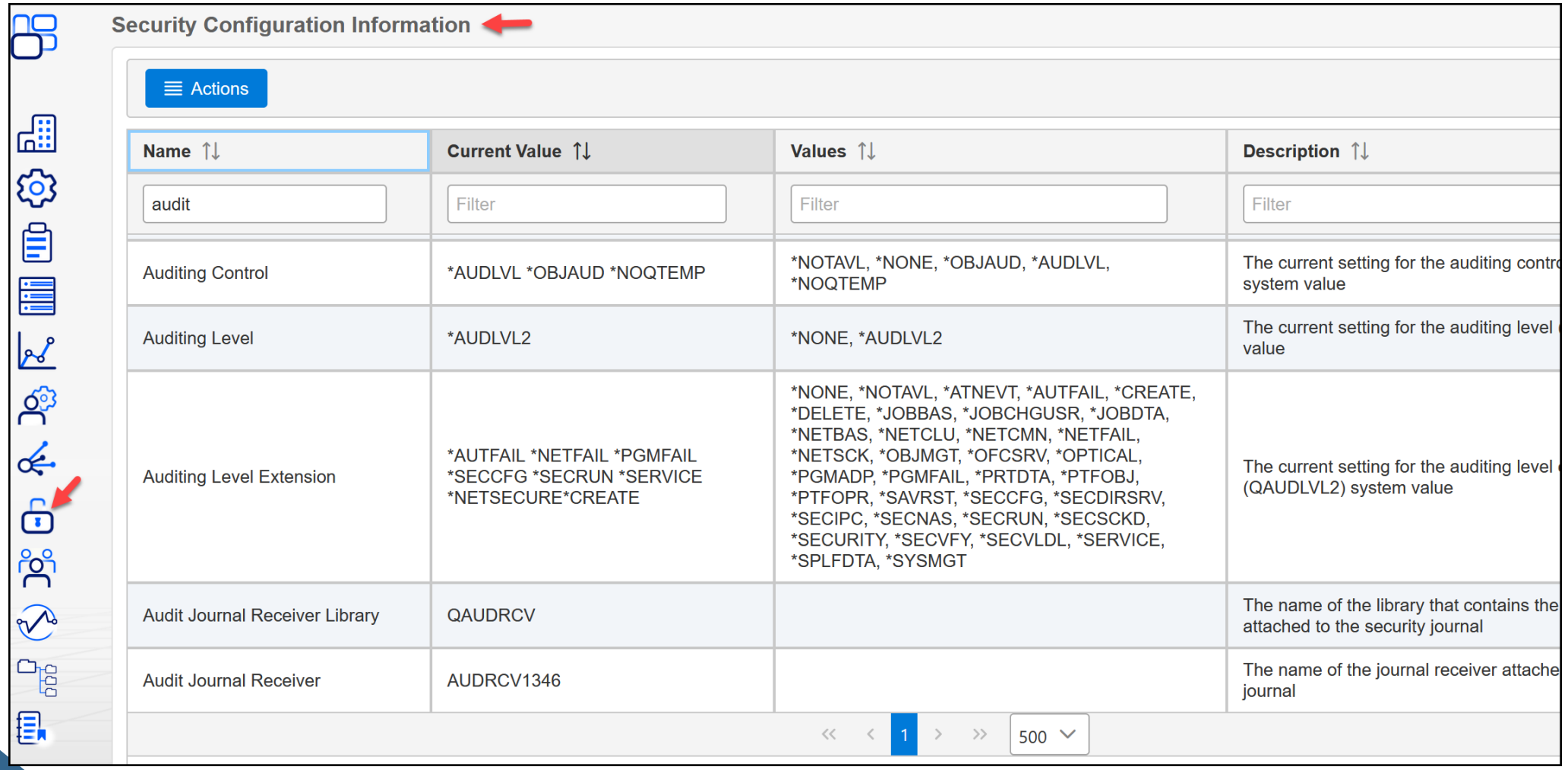
kisco

System Value Recommendations

System Value	Change if Set to	Recommended Setting
QSECURITY	< 40	40 or 50
QPWDLVL	0, 1, 2	3 if IBM i 7.4 4 if IBM i 7.5
QPWDRULES	*PWDSYSVAL	*MINLEN14, *MAXLEN128, *REQANY3, *LMTPRFNAME, *ALLCRTCHG
QPWDEXPITV	*NOMAX	It depends … often 60-90 but using passphrases 180-365
QMAXSIGN	*NOMAX	3-5
QCRTAUT	*ALL	Anything but *ALL! *CHANGE is better, *USE is better yet. *EXCLUDE is great Use the CRTAUT parm at the library level for more granular control
QSSL*	Protocols < TLS1.2	*OPSYS (depending on the OS release) or *TLS1.2 and/or TLS1.3
QAUDCTL	*NONE	*AUDLVL, *OBJAUD, *NOQTEMP
QAUDLVL	*NONE	*AUTFAIL, *CREATE, *DELETE, *SAVRST,*PTFOPR, *SERVICE, *SECCFG, *SECRUN (or *SECURITY) Optional: *PGMFAIL (if < 40), *ATNEVT, *JOBBAS

kisco

Working with System Values



http://your_system_name:2002/Navigator/login

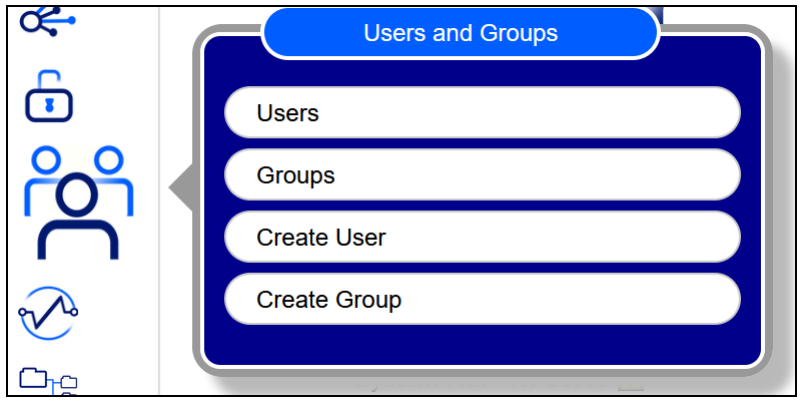
Perform a User Profile Checkup

Reviewing User Profile Capabilities

- **Group assignments** need to be reviewed periodically (e.g. quarterly)
  - DSPUSRPRF USRPRF(QPGMR) TYPE(*GRPMBR)
  - DSPAUTUSR SEQ(*GRPPRF)
- **Special authorities**
  - Create new profiles with only the special authorities required to do their jobs
  - PRTUSRPRF
  - DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(MY_LIB/PROFILES)
  - QSYS2.USER_INFO view
- **Limited capability** setting
  - Most users should be LMTCPB(*YES)

kisco

Users (or Groups) – Navigator for i



IBM Navigator for i

Search common1 cwoodbury

Users

Actions

Name	Profile Status	Special Authorities	Description	Group	Supplemental Groups	Profile Type	NetServer Disabled
c	Filter	*ALLOBJ	Filter	Filter	Filter	Filter	Filter
CWOODBURY2	*ENABLED	*ALLOBJ		*NONE		User	NO
CGUARINO	*DISABLED	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG	Charles Guarino - Demo Presenter	*NONE		User	NO
CGUARINO1	*DISABLED	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG	Charles Guarino - Demo Presenter	*NONE		User	NO

kisco

List the Members of Each Group Profile

```
 8  --
 9  -- List members of each group profile
10  --
11  SELECT *
12     FROM QSYS2.group_profile_entries;
13  stop;
```

Group Profile Name GROUP_PROFILE_NAME	User Profile Name USER_PROFILE_NAME	User Text USER_TEXT
ACGRPPRF	AAATIM4	asdfasdf
ACGRPPRF	ACUSER04	Test user for authority collection
ADMIN_G21	AAATIM4	asdfasdf
ALLOBJTEAM	SCOTTF	Scott Forstie
APACHEGRP	APACHE001	REQUIRED FOR APACHE SERVER LAB

Notes:

- Launch Access Client Solutions (ACS) -> Run SQL Scripts
- Lists the profile whether the group is the first group or a supplemental group
- Right-click to download to a spreadsheet
- All IBM i services are listed here: https://www.ibm.com/support/pages/node/1119123

kisco

Special Authority Analysis using QSYS2.USER_INFO

```
17  -- Special Authority analysis. This version lists all profiles with *ALLOBJ assigned - either to the profile itself or to one of its groups.
18  -- Works for all special authorities. Simply substitute all instances of *ALLOBJ for another special authority
19  --
20  select user_name, special_authorities, group_profile_name, supplemental_group_list, text_description
21   from QSYS2.USER_INFO
22   where SPECIAL_AUTHORITIES like '%*ALLOBJ%' or
23        AUTHORIZATION_NAME in (select USER_PROFILE_NAME
24           from QSYS2.GROUP_PROFILE_ENTRIES
25           where GROUP_PROFILE_NAME in (select AUTHORIZATION_NAME
26                from QSYS2.USER_INFO
27                where SPECIAL_AUTHORITIES like '%*ALLOBJ%'))
28   order by AUTHORIZATION_NAME;
29  stop;
```

Authorization Name USER_NAME	Special Authorities SPECIAL_AUTHORITIES	Group Profile Name GROUP_PROFILE_NAME	Supplemental Group List SUPPLEMENTAL_GROUP_LIST	Text Description TEXT_DESCRIPTION
AARONC	*ALLOBJ *SECADM *JOBCTL *SPLCTL ...	*NONE	-	-
ACADMN01	*ALLOBJ *SECADM	*NONE	-	Admin user for authority collection
ACADMN02	*ALLOBJ *SECADM	*NONE	-	Admin user for authority collection
ACADMN03	*ALLOBJ *SECADM	*NONE	-	Admin user for authority collection

For assistance:

- ACS -> Run SQL Scripts
- Edit -> Examples -> Insert from Examples. Use drop down to switch to IBM i Services

kisco

Profiles with a Default Password

```
38  --  Find user profiles with default passwords (password same as the user profile name)
39  --
40  select USER_NAME, STATUS, PASSWORD_EXPIRATION_INTERVAL, SPECIAL_AUTHORITIES, GROUP_PROFILE_NAME,
41        SUPPLEMENTAL_GROUP_LIST, LAST_USED_TIMESTAMP, CREATION_TIMESTAMP, USER_CREATOR,
42        TEXT_DESCRIPTION
43    from qsys2.user_info
44    where USER_DEFAULT_PASSWORD = 'YES'
45    order by status;
```

Authorization Name USER_NAME	Status STATUS	Password Expiration Interval PASSWORD_EXPIRATION_INTERVAL	Special Authorities SPECIAL_AUTHORITIES	Group Profile Name GROUP_PROFILE_NAME	Supplemental Group List SUPPLEMENTAL_GROUP_LIST	Last Used Timestamp LAST_USED_TIMESTAM
AWONT	*DISABLED	0	*ALLOBJ	*NONE	-	-
BEDROCK02	*DISABLED	0	-	*NONE	-	-
BOAT	*DISABLED	0	-	*NONE	-	-
CHRISD	*DISABLED	0	*SECADM	*NONE	-	-
GENIEUSR01	*DISABLED	0	-	QPGMR	-	-
LABGIT	*DISABLED	0	-	*NONE	-	2020-09-16 00:00:00.000

Hints:

- Use this method to perform other analysis on user profile configuration. For example:
  - Profiles not limited *YES (not LMTCPB(*YES))
  - Profiles with a non-expiring password (PWDEXPITV(*NOMAX))
- Include (or remove) the other attributes selected so it makes sense for your reporting / analysis

kisco

Easily Send Output to a Spreadsheet and Email

```
93  VALUES SYSTOOLS.GENERATE_SPREADSHEET(
94   PATH_NAME       => '/home/cwoodbury/userinfo',
95   SPREADSHEET_QUERY =>
96   'SELECT *
97    FROM qsys2.user_info
98    WHERE no_password_indicator = "YES"
99        AND password_expiration_interval = "-1"
100   ORDER BY authorization_name',
101  SPREADSHEET_TYPE  => 'csv',
102  COLUMN_HEADINGS   => 'NONE'
103 );
104
```

```
00001
    1
```

```
114 --
115 -- One time setup - user has to be an SMTP user - no need to run if already enrolled
116 call qsys2.qcmdexc('QSYS/ADDUSRSMTP  USRPRF(' concat user concat ')');
117 stop;
118
119 VALUES SYSTOOLS.SEND_EMAIL(
120  TO_EMAIL   => 'carol@dxrsecurity.com',
121  SUBJECT    => 'Profiles config info ' concat (select host_name from sysibmadm.env_sys_info),
122  BODY       => 'Users without a password but password expiration nomax. Captured on  ' concat current timestamp,
123  ATTACHMENT => '/home/cwoodbury/userinfo.csv'
124 );
125 stop;
```

Examples from Edit-> Examples->
Insert from Examples->SYSTOOLS

kisco

Listing Inactive Profiles with SQL

```
46  --
47  --  List User profiles that haven't been used in the last 3 months
48  --
49  SELECT user_name,
50        date(last_used_timestamp) as last_used,
51        timestamp(previous_signon, 0) as last_signon,
52        timestamp(creation_timestamp, 0) as create_time,
53        status,
54        text_description
55     FROM QSYS2.USER_INFO
56     WHERE (last_used_timestamp IS NULL
57           OR last_used_timestamp < CURRENT TIMESTAMP - 3 MONTHS)
58        AND (creation_timestamp < CURRENT TIMESTAMP - 3 MONTHS);
```

Authorization Name USER_NAME	LAST_USED	LAST_SIGNON	CREATE_TIME	Status STATUS	Text Description TEXT_DESCRIPTION
#GNOTEST	-	-	2022-01-03 09:07:31	*ENABLED	-
AAATIM4	-	-	2021-07-07 09:01:55	*ENABLED	asdfasdf
AARONC	2020-03-11	2020-03-11 09:03:36	2019-05-06 14:17:45	*ENABLED	-
AATIM	-	-	2018-08-27 07:41:53	*ENABLED	Setsrgee
AATIM3	-	-	2022-10-21 13:18:20	*ENABLED	Test users
ACADMN01	2020-09-15	2020-09-15 16:15:08	2019-05-02 17:05:31	*ENABLED	Admin user for authority collection

Make sure you're looking at the right date. Last used, NOT last signon!

Managing Inactive Profiles with an SQL

```
62  --  DISABLE User profiles that haven't been used in the last 3 months
63  -- To ensure a profile is not disabled, add it to an omission list (file QASECIDL) by running CHGACTPRFL (Change Active Profile List).
64  -- (The list ships populated with the IBM-supplied profiles.)
65  --
66  SELECT cup.*
67     FROM QSYS2.USER_INFO u,
68        TABLE (
69           SYSTOOLS.CHANGE_USER_PROFILE(P_USER_NAME => USER_NAME, P_STATUS => '*DISABLED', PREVIEW => 'YES')
70        ) cup
71     WHERE (u.user_name NOT IN (SELECT aidprf
72                   FROM QSYS.QASECIDL))
73        AND ((last_used_timestamp IS NULL
74              OR last_used_timestamp < CURRENT TIMESTAMP - 3 MONTHS)
75           AND (creation_timestamp < CURRENT TIMESTAMP - 3 MONTHS));
76  stop;
```

USER_NAME	CHANGE_ATTEMPTED	CHANGE_SUCCESSFUL	CHGUSRPRF_COMMAND	FAILURE_MESSAGE
#GNOTEST	NO	-	QSYS/CHGUSRPRF USRPRF(#GNOTEST) STATUS(*DISABLED)	-
AAATIM4	NO	-	QSYS/CHGUSRPRF USRPRF(AAATIM4) STATUS(*DISABLED)	-
AARONC	NO	-	QSYS/CHGUSRPRF USRPRF(AARONC) STATUS(*DISABLED)	-
AATIM	NO	-	QSYS/CHGUSRPRF USRPRF(AATIM) STATUS(*DISABLED)	-
AATIM3	NO	-	QSYS/CHGUSRPRF USRPRF(AATIM3) STATUS(*DISABLED)	-

Preview => ‘YES’ lists the profiles
Preview => ‘NO’ disables the profiles

Deleting User Profiles using SQL

```
--
--  description: Delete User profiles that are at least 6 months old and have not been
--               used in the last six months
--               Reassign ownership of any object to the user's first group profile
--               If the user has no group, reassign object ownership to CAROL
--               If the user profile is in the "do not delete list" (file QUSRSYS.QASECIDL), skip it
--
SELECT qsys2.qcmdexc('DLTUSRPRF USRPRF(' concat user_name concat ') '
                concat 'OWNOBJOPT(*CHGOWN ' concat
                case GROUP_PROFILE_NAME when '*NONE' then 'CAROL'
                  else GROUP_PROFILE_NAME end concat ')' )
    FROM QSYS2.USER_INFO u
    WHERE (coalesce(last_used_timestamp, previous_signon, current timestamp - 7 months)
             < CURRENT TIMESTAMP - 6 MONTHS)
      AND (creation_timestamp < CURRENT TIMESTAMP - 6 MONTHS)
      AND (user_creator not in ('*IBM', 'QLPINSTALL', 'QSYS', 'QSECOFR'))
      AND u.user_name not in (select aidprf from QUSRSYS.QASECIDL);
```

SQL courtesy of Scott Forstie

kisco

Use of IBM-Supplied Profiles

- QSECOFR should only be used to upgrade the operating system, apply PTFs or use vendor products that won't work otherwise.
  - Must have a password but can be set to STATUS(*DISABLED)
- QPGMR should never be used for sign on and is discouraged even as a group profile
  - Should be password - *NONE
- QSYSOPR should not be used for sign on but may be used as a group
  - Should be password - *NONE
- QSRV and QSRVBAS will be used to service the system
  - Should be password - *NONE
- QUSER should not be used for sign on or as a group profile.
  - Should be password - *NONE
  - Cannot be set to status *DISABLED

kisco

Service Account Setting Recommendations

- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible. Do not default to *ALLOBJ!
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)
  - TEXT(‘Something informative’)
  - PASSWORD -> Not a default!
  - PWDEXPITV -> Recommend the pwd be changed periodically

➡ Add rules in exit point products to stop these profiles from being used for other purposes.

kisco

Groups / Ownership Account Setting Recommendations

- Create the profile with the following attributes:
  - SPCAUT(*NONE) – where possible
  - PASSWORD(*NONE)
  - PWDEXPITV(*SYSVAL)
  - STATUS(*DISABLED)
  - LMTCPB(*YES)
  - INLPGM(*NONE)
  - INLMNU(*SIGNOFF)
  - ATNPGM(*NONE)
  - TEXT(‘Give a meaningful and informative description!’)

kisco

Protect Your Data

Now, More than Ever, Data Must be Protected… Why?

- Data has value to your organization!

- Ransomware
- Other bad actors
- Insider threat

- AI!!!!
  - AI leakage
  - AI poisoning

Data May be in Either a Library or a Directory

- Data should be secured
  - For Integrity ->
    - *PUBLIC(*USE) for objects in a library
    - *PUBLIC DTAAUT(*RX) OBJAUT(*NONE) for objects in a directory
  - For Confidentiality ->
    - *PUBLIC(*EXCLUDE)
    - *PUBLIC DTAAUT(*EXCLUDE) OBJAUT(*NONE)
- Use Authority Collection to determine how much authority is required.

kisco

To Review Object Authorities

- QSYS2.object_privileges (same as the DSPOBJAUT command)
- QSYS2.ifs_object_privileges (same as the DSPAUT command)
- QSYS2.object_ownership (same as the WRKOBJOWN command or “QSYLOBJA” API)

kisco

Analyze Objects in a Specific Library

```
84  --
85  -- description: Find PROD_LIB/*ALL *FILE objects that don't have the proper object authorities
86  --
87  select *
88    from qsys2.object_privileges
89    where system_object_schema = 'PROD_LIB' and
90          object_type = '*FILE' and
91          ((authorization_name = '*PUBLIC' and object_authority <> '*AUTL') or
92            authorization_list <> 'PRODAUTL' or
93            owner <> 'PROD_OWNER');
94  stop;
95
```

Object Schema OBJECT_SCHEMA	Object Name OBJECT_NAME	System Object Schema SYSTEM_OBJECT_SCHEMA	System Object Name SYSTEM_OBJECT_NAME	Object Type OBJECT_TYPE	SQL Object Type SQL_OBJECT_TYPE	Authorization Name AUTHORIZATION_NAME	Object Authority OBJECT_AU
PROD_LIB	OVERDUE	PROD_LIB	OVERDUE	*FILE	TABLE	*PUBLIC	*AUTL
PROD_LIB	OVERDUE	PROD_LIB	OVERDUE	*FILE	TABLE	CWOODBURY	*ALL
PROD_LIB	PAYABLES	PROD_LIB	PAYABLES	*FILE	TABLE	*PUBLIC	*AUTL
PROD_LIB	PAYABLES	PROD_LIB	PAYABLES	*FILE	TABLE	CWOODBURY	*ALL
PROD_LIB	RECEIVABLE	PROD_LIB	RECEIVABLE	*FILE	-	*PUBLIC	*AUTL
PROD_LIB	RECEIVABLE	PROD_LIB	RECEIVABLE	*FILE	-	CWOODBURY	*ALL

kisco

Analyze Objects in a Directory

```
174 --
175 -- description: Find any files under an IFS path that have the wrong value for owner or *PUBLIC
176 --
177 with ifs_auts as (
178    select path_name from table(
179         qsys2.ifs_object_statistics(start_path_name => '/payroll_upload', IGNORE_ERRORS => 'YES')
180  ))
181  select iop.*
182    from ifs_auts, table(qsys2.ifs_object_privileges(path_name)
183         ) iop
184    where owner <> 'PROD_OWNER' or
185         (OBJECT_TYPE = '*DIR' and
186           authorization_name = '*PUBLIC' and
187           data_authority <> '*EXCLUDE');
188 stop;
```

PATH_NAME	OBJECT_TYPE	OWNER	PRIMARY_GROUP	AUTHORIZATION_LIST	AUTHORIZATION_NAME	DATA_AUTHORITY
/payroll_upload	*DIR	CWOODBURY	-	-	*PUBLIC	*EXCLUDE

kisco

List Objects Secured by an Authorization List

```
135 -- description: List objects secured with a specific authorization list
136 --
137 SELECT authorization_list,
138        object_schema,
139        object_name,
140        system_object_type,
141        object_owner,
142        path_name
143    FROM qsys2.authorization_list_info
144    WHERE authorization_list = 'AR_AUTL';
145 stop;
```

Authorization List	Object Schema	Object Name	System Object Type	Object Owner	Path Name
AUTHORIZATION_LIST	OBJECT_SCHEMA	OBJECT_NAME	SYSTEM_OBJECT_TYPE	OBJECT_OWNER	PATH_NAME
AR_AUTL	CWOODBURY	TESTMBRAUT	*FILE	CWOODBURY	-
AR_AUTL	PROD_LIB	AP	*PGM	CWOODBURY	-
AR_AUTL	PROD_LIB	AR	*PGM	CWOODBURY	-
AR_AUTL	PROD_LIB	FINANCE	*PGM	CWOODBURY	-

QSYS2.AUTHORIZATION_LIST_INFO: lists the objects secured by an authorization list

QSYS2.AUTHORIZATION_LIST_USER_INFO: lists the users authorized to an authorization list

kisco

Find Programs that Adopt a Powerful User QSYS2.program_info

```
205 -- List the programs that adopt QSECOFR
206 --
207 SELECT *
208    FROM qsys2.program_info
209    WHERE user_profile = '*OWNER'
210         AND owner = 'QSECOFR'
211    ORDER BY program_library;
212 stop;
```

Program Library PROGRAM_LIBRARY	Program Name PROGRAM_NAME	Program Type PROGRAM_TYPE	Object Type OBJECT_TYPE	Create Timestamp CREATE_TIMESTAMP	Text Description TEXT_DESCRIPTION	Program Owner PROGRAM_OWNER
EMSANDBOX	USERENV	ILE	*PGM	2014-07-11 01:24:01	Set up user environment f...	QSECOFR
PROD_LIB	INLMENU	OPM	*PGM	2020-08-10 12:23:01	-	QSECOFR
PROFOUNDUI	PUILICR	ILE	*PGM	2018-03-05 11:25:07	-	QSECOFR
PROFOUNDUI	PUIDFINIT	ILE	*SRVPGM	2018-03-05 11:18:26	-	QSECOFR

kisco

Analyze the Audit Journal

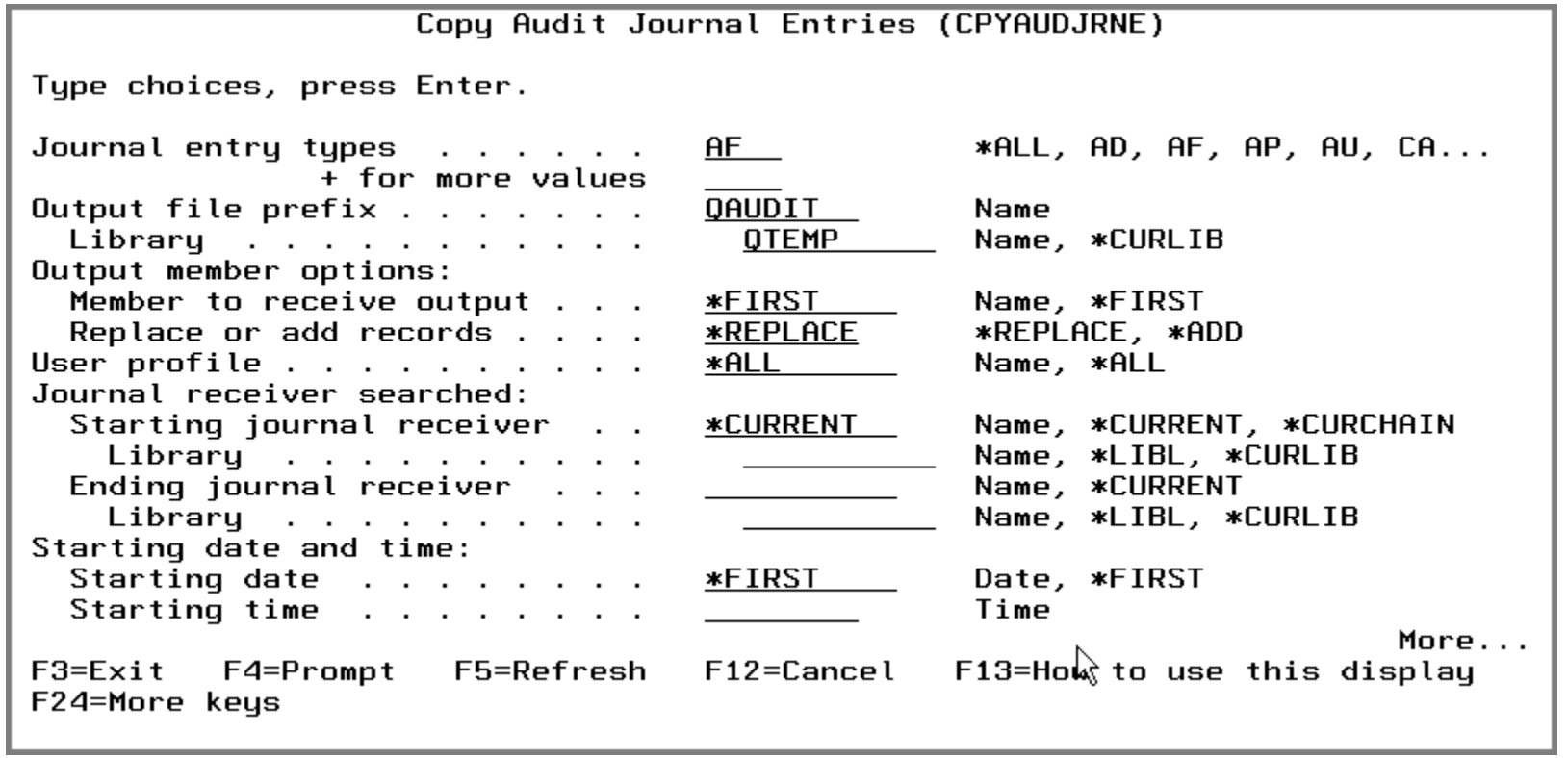
Examples of Actions to Review

- Changes to System Values (SV)
- Selected changes to User Profiles (CP)
- Changes to permissions for selected objects (CA)
- Commands run (CD)

kisco

Copy Audit Journal Entries (CPYAUDJRNE)

Creates a file named QAUDITxx where xx is the journal entry type



Hint: Press F1 on the Journal entry types field for a description of two-letter types

Audit Journal Entry SQL Table Functions

- Table functions to parse out the detailed information of the following audit journal entries:
  - AF – Authority Failure (SYSTOOLS.AUDIT_JOURNAL_AF)
  - CA – Changes to Authority (SYSTOOLS. AUDIT_JOURNAL_CA)
  - OW – Ownership Changes (SYSTOOLS. AUDIT_JOURNAL_OW)
  - PW – Password (SYSTOOLS. AUDIT_JOURNAL_PW)
  - Many more…
- Available starting in V7R3 TR10 and V7R4 TR4
  - https://www.ibm.com/docs/en/i/7.5?topic=services-audit-journal-entry

kisco

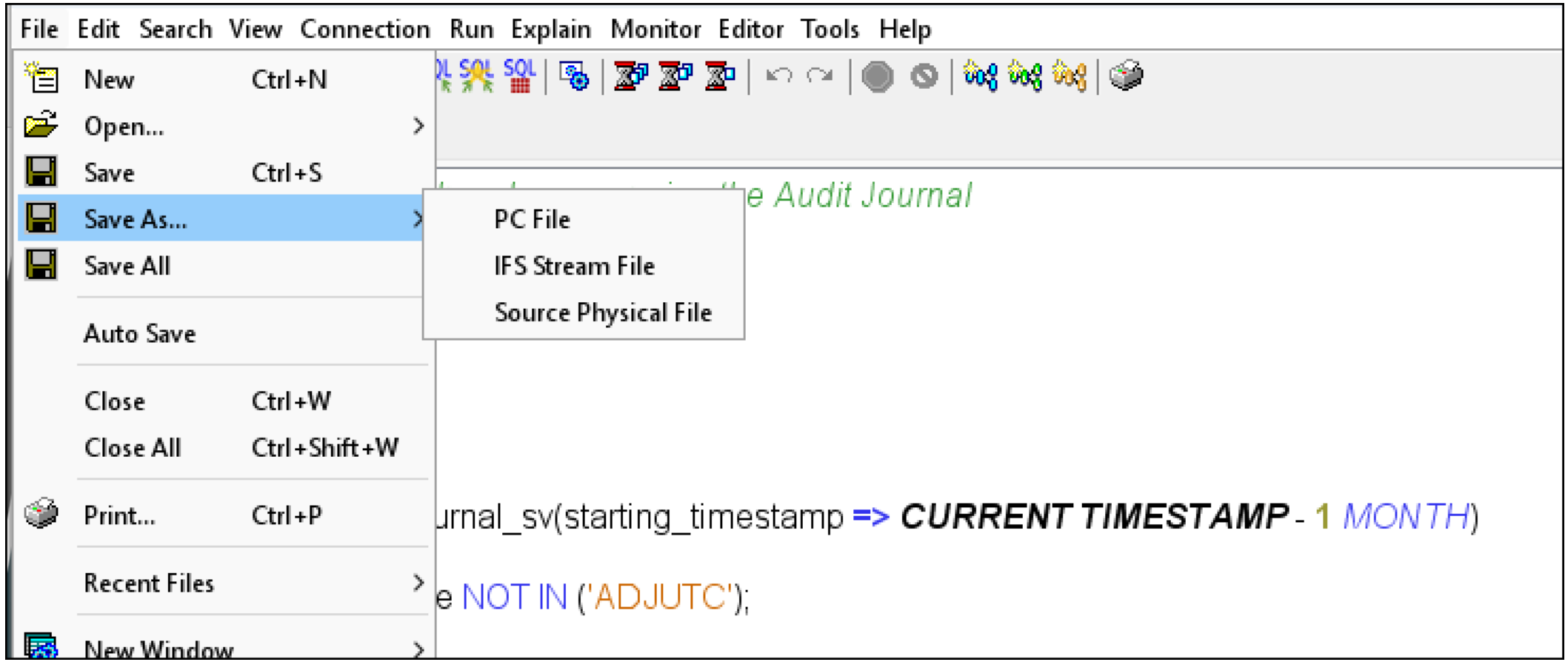
Find SysVal Changes via the Audit Journal

```
181 --
182 select entry_timestamp, qualified_job_name, user_name, system_value, new_value, old_value
183   from table (
184       systools.audit_journal_sv(STARTING_TIMESTAMP => current timestamp - 1 month
185       )
186     )
187   where system_value not in ('ADJUTC');
188 stop;
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	USER_NAME	SYSTEM_VALUE	NEW_VALUE
2023-07-26 15:32:31.571376	019538/QUSER/QZRCSRVS	LRPOWELL	QAUDLVL2	*NONE
2023-07-26 15:32:31.572160	019538/QUSER/QZRCSRVS	LRPOWELL	QAUDLVL	*ATNEVT *AUTFAIL *CREATE *DELETE
2023-07-27 14:18:45.931472	041856/QUSER/QZRCSRVS	CWOODBURY	QAUDLVL2	*NONE

kisco

Save your SQL!



kisco

Add SQL into a CL Program, then Schedule

```
PGM    /* PROGRAM PROVIDED AS-IS WITH NO WARRANTY */

/* DELETE THE TEMPORARY OUTPUT FILE */
DLTF QTEMP/SYSVALCHGS
MONMSG MSGID(CPF2105)

/* RECREATE THE OUTPUT FILE WITH NEW DATA */
RUNSQL SQL('CREATE TABLE QTEMP.SYSVALCHGS AS                    +
 (SELECT ENTRY_TIMESTAMP, QUALIFIED_JOB_NAME,                   +
         USER_NAME, NEW_VALUE, OLD_VALUE                        +
    FROM TABLE (SYSTOOLS.AUDIT_JOURNAL_SV(                      +
         STARTING_TIMESTAMP => CURRENT TIMESTAMP - 7 DAYS )) +
    WHERE SYSTEM_VALUE NOT IN (''ADJUTC'')) WITH DATA')      +
       COMMIT(*NONE) NAMING(*SQL)
MONMSG MSGID(SQL9010)

/* GENERATE A SPOOLED FILE REPORT */
RUNQRY QRYFILE((QTEMP/SYSVALCHGS)) OUTTYPE(*PRINTER)
MONMSG MSGID(QRY1210)

ENDPGM
```

kisco

CP Entries

```
76  --
77  -- Get specific fields to determine who changed the DEVELOPER profile
78  --
79  SELECT entry_timestamp,
80        qualified_job_name,
81        user_name AS CHANGER,
82        user_profile AS PROFILE_CHANGED,
83        program_library,
84        program_name,
85        special_authorities,
86        previous_special_authorities
87     FROM TABLE (
88           systools.audit_journal_cp(starting_timestamp => CURRENT TIMESTAMP - 7 DAYS)
89         )
90     WHERE user_profile = 'DEVELOPER'
91     ORDER BY entry_timestamp;
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	CHANGER	PROFILE_CHANGED	PROGRAM_LIBRARY	PROGRAM_NAME	SPECIAL_AUTHORITIES	PREVIOUS_SPECIAL_AUTH
2023-09-19 13:18:04....	392252/CWOOD...	CWOODBURY	DEVELOPER	QSYS	QCMD	-	-
2023-09-20 14:21:49....	415662/CWOOD...	CWOODBURY	DEVELOPER	QSYS	QCMD	*ALLOBJ	-

kisco

Displaying Commands Run by a User

```
193 SELECT program_library,
194        program_name,
195        object_library,
196        object_name,
197        where_run,
198        where_run_detail,
199        command_string
200     FROM TABLE (
201             systools.audit_journal_cd(starting_timestamp => CURRENT TIMESTAMP - 7 days)
202          )
203     WHERE user_name = 'CWOODBURY';
204 stop;
```

PROGRAM_LIBRARY	PROGRAM_NAME	OBJECT_LIBRARY	OBJECT_NAME	WHERE_RUN	WHERE_RUN_DETAIL
QSYS	QCMD	QSYS	QSH	B	In a batch job but not for any of the reason listed under Y,
QSYS	QCMD	QSHELL	QSH	B	In a batch job but not for any of the reason listed under Y,
QSYS	QP0ZSPWT	QSYS	OVRPRTF	E	The command string was passed as a parameter to one of
QSYS	QP0ZSPWT	QSYS	CALL	E	The command string was passed as a parameter to one of
QSYS	QP0ZSPWT	QSYS	DLTOVR	E	The command string was passed as a parameter to one of
QSYS	QP0ZSPWT	QSYS	CHGJOB	E	The command string was passed as a parameter to one of

kisco

Document Profiles Deleted

```
188 --
189 --  Document the profiles deleted in the last week
190 --
191 SELECT entry_timestamp,
192        qualified_job_name,
193        user_name AS deleter,
194        program_library,
195        program_name,
196        object_name AS profile_deleted
197     FROM TABLE (
198            systools.audit_journal_do(starting_timestamp => CURRENT TIMESTAMP - 7 DAYS)
199          )
200     WHERE object_type = '*USRPRF'
201     ORDER BY entry_timestamp;
202 stop;
```

ENTRY_TIMESTAMP	QUALIFIED_JOB_NAME	DELETER	PROGRAM_LIBRARY	PROGRAM_NAME	PROFILE_DELETED
2023-08-25 17:36:08.568752	501940/CWOODBURY/QPADEV0005	CWOODBURY	QSYS	QCMD	DUMMY

kisco

Audit Journal Entries to Send to Your SIEM

- PW
  - ‘U’ entries where the User is “root” or “Admin” and attempt originates from outside of the organization
  - ‘P’ entries where many occur within a short period of time and for the well-known IBM i-supplied profiles (QSYS, QSECOFR, QUSER, QSYSOPR, QPGMR, QSRV, QSRVBAS)
- JS
  - Job start entries that originate from an unknown external IP address
  - Job starts for unknown entries (such as QSECOFR)
- CP
  - Password changes for QSECOFR and other IBM-supplied profiles
  - Re-enablement of QSECOFR (if kept STATUS *DISABLED)
- VP
  - Invalid password attempts via NetServer
- IM – Intrusion detection events
  - Malware detection
  - Denial of service attacks
- AF - Authority failures to sensitive files

kisco

Audit Journal Receivers

- Review how audit journal receivers are saved
- Ensure you have a contiguous range
- Save so you can restore by date

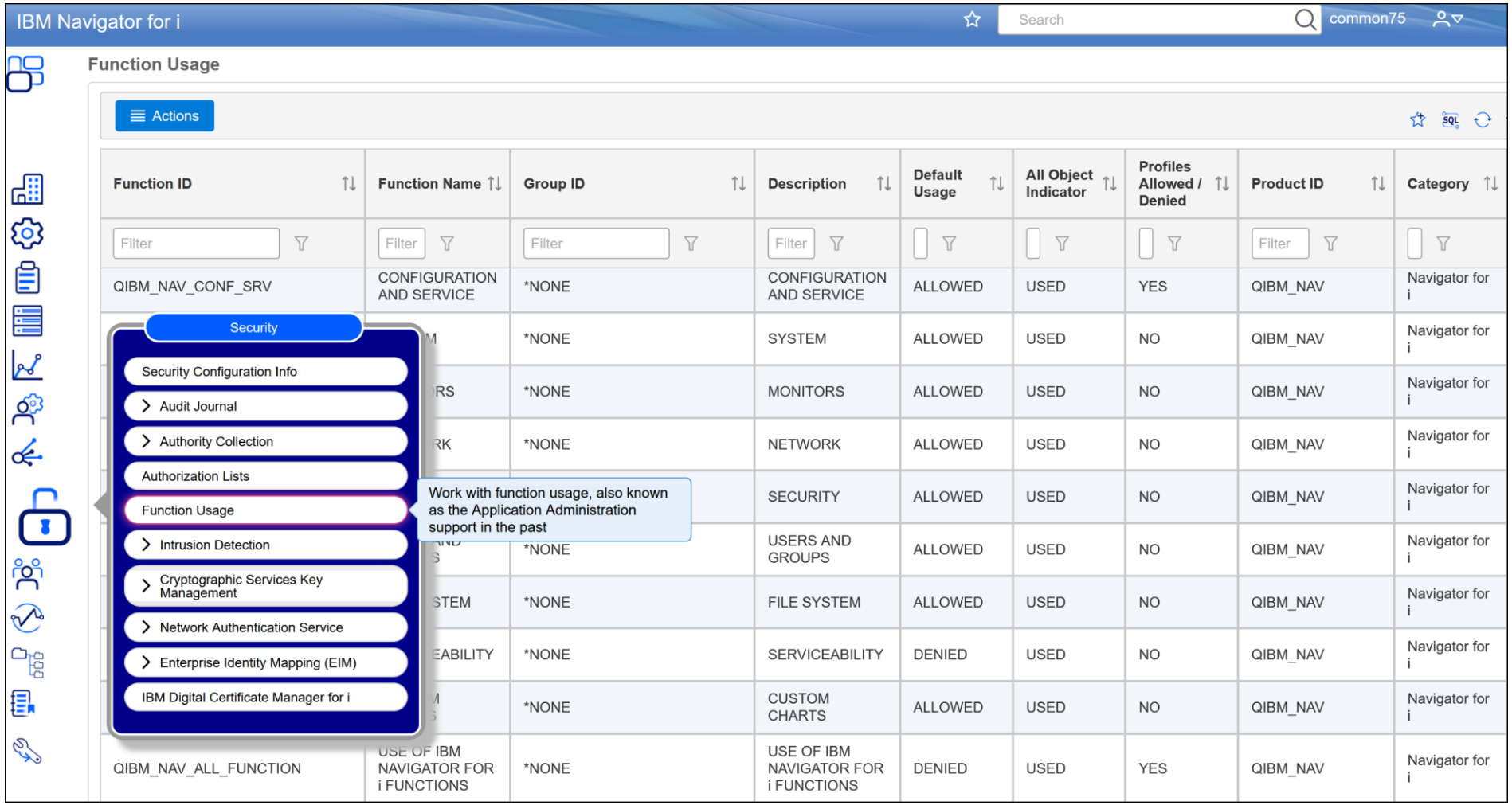
Review Function Usage Configuration

Function Usage (aka Application Administration)

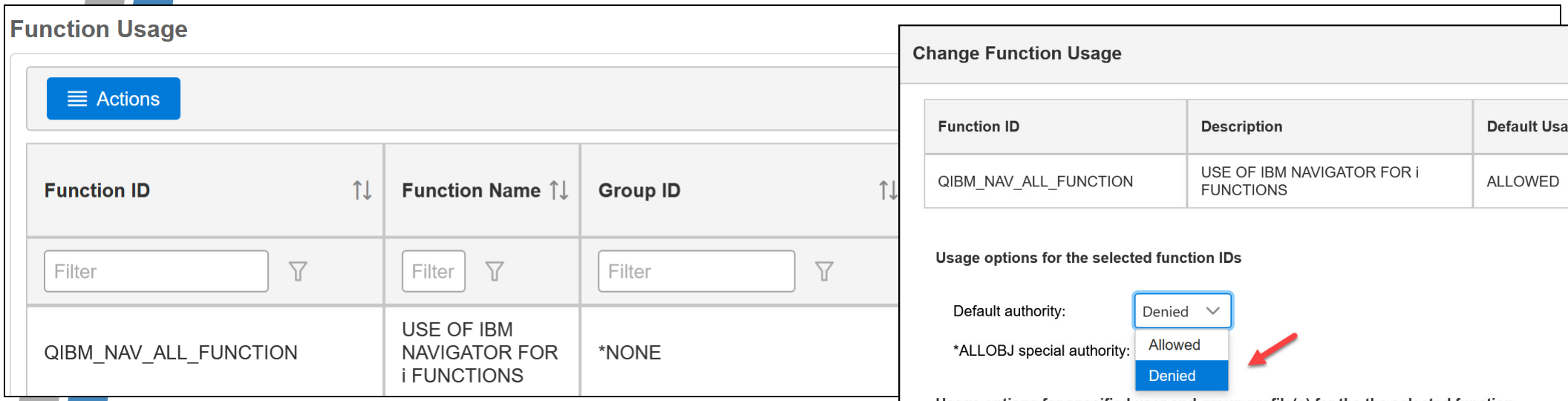
- Allows you to control access to:
  - Navigator for i features
  - Access Client Solutions (ACS) features (Data Transfer, Run SQL Scripts, etc)
  - Host functions (Access the joblog of an *ALLOBJ user, DDM, etc)

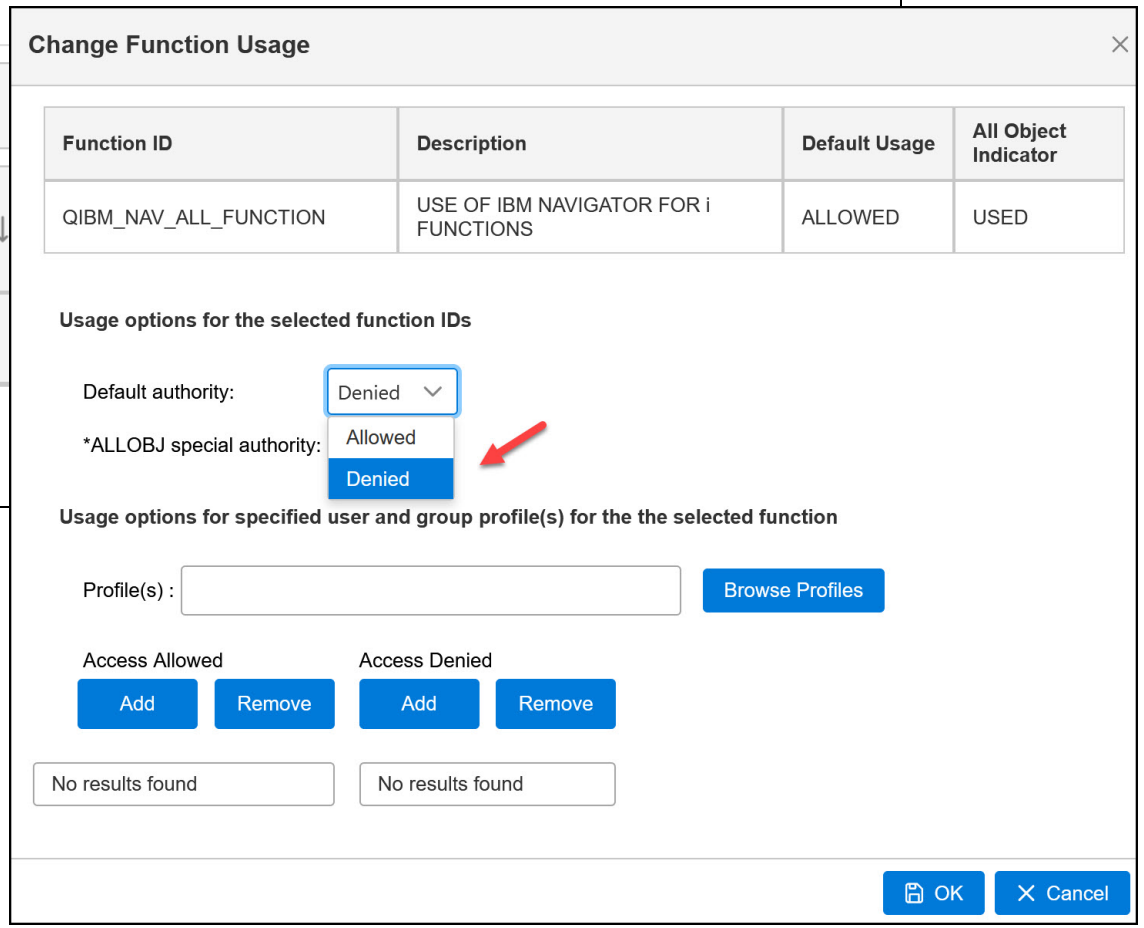
kisco

Application Administration: (Function Usage) in New Nav



Define Who Can Access (new) Navigator for i

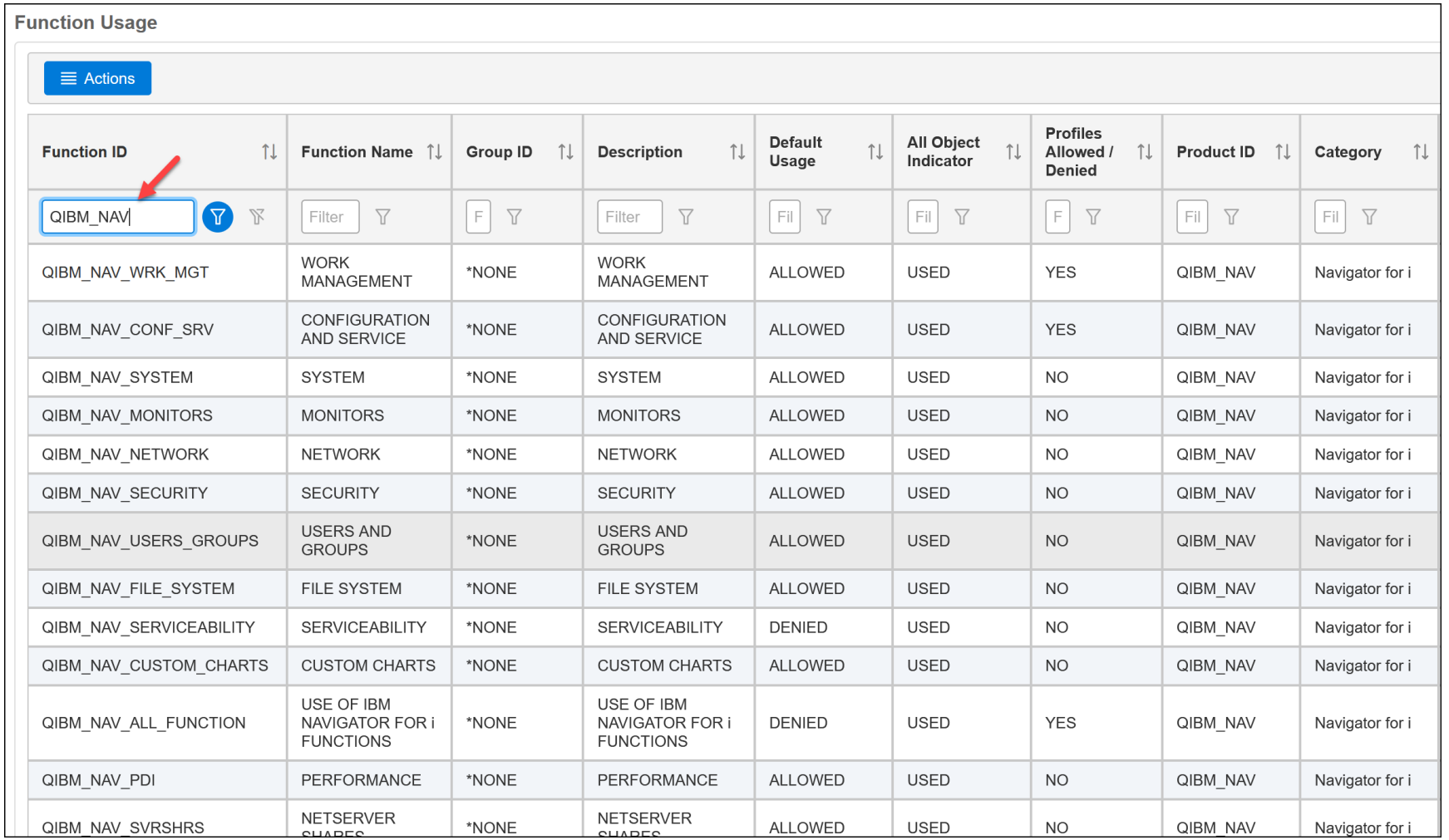




- MUST re-define Nav for i settings !!!
- ACS and Host functions remain as they did from Heritage Nav

kisco

Review Access to Navigator for i Features (QIBM_NAV)



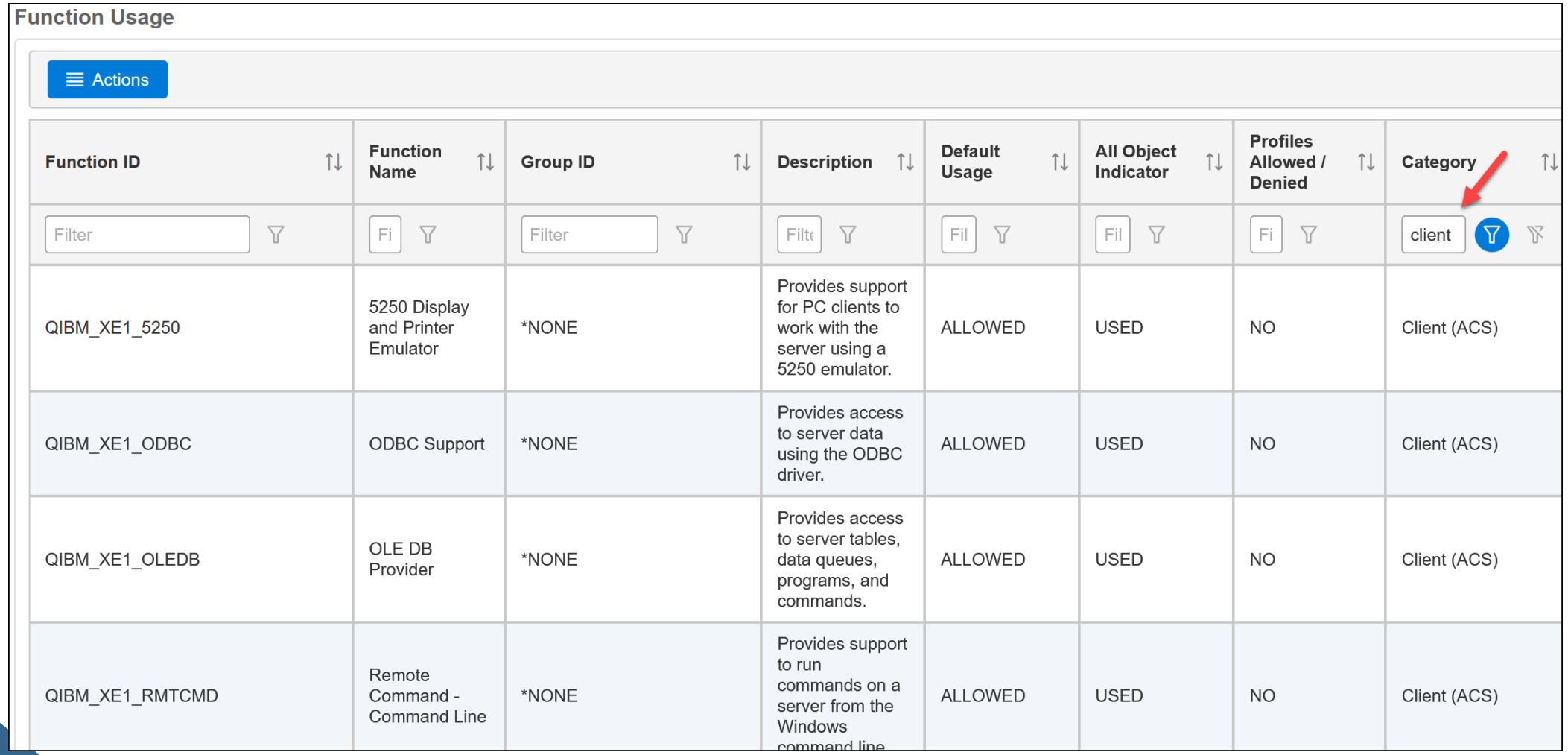
Function Usage

Actions

Function ID	Function Name	Group ID	Description	Default Usage	All Object Indicator	Profiles Allowed / Denied	Product ID	Category
QIBM_NAV	Filter	F	Filter	Fil	Fil	F	Fil	Fil
QIBM_NAV_WRK_MGT	WORK MANAGEMENT	*NONE	WORK MANAGEMENT	ALLOWED	USED	YES	QIBM_NAV	Navigator for i
QIBM_NAV_CONF_SRV	CONFIGURATION AND SERVICE	*NONE	CONFIGURATION AND SERVICE	ALLOWED	USED	YES	QIBM_NAV	Navigator for i
QIBM_NAV_SYSTEM	SYSTEM	*NONE	SYSTEM	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_MONITORS	MONITORS	*NONE	MONITORS	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_NETWORK	NETWORK	*NONE	NETWORK	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_SECURITY	SECURITY	*NONE	SECURITY	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_USERS_GROUPS	USERS AND GROUPS	*NONE	USERS AND GROUPS	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_FILE_SYSTEM	FILE SYSTEM	*NONE	FILE SYSTEM	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_SERVICEABILITY	SERVICEABILITY	*NONE	SERVICEABILITY	DENIED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_CUSTOM_CHARTS	CUSTOM CHARTS	*NONE	CUSTOM CHARTS	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_ALL_FUNCTION	USE OF IBM NAVIGATOR FOR i FUNCTIONS	*NONE	USE OF IBM NAVIGATOR FOR i FUNCTIONS	DENIED	USED	YES	QIBM_NAV	Navigator for i
QIBM_NAV_PDI	PERFORMANCE	*NONE	PERFORMANCE	ALLOWED	USED	NO	QIBM_NAV	Navigator for i
QIBM_NAV_SVRSHRS	NETSERVER SHARES	*NONE	NETSERVER SHARES	ALLOWED	USED	NO	QIBM_NAV	Navigator for i

kisco

Define Access to ACS Features (Client)

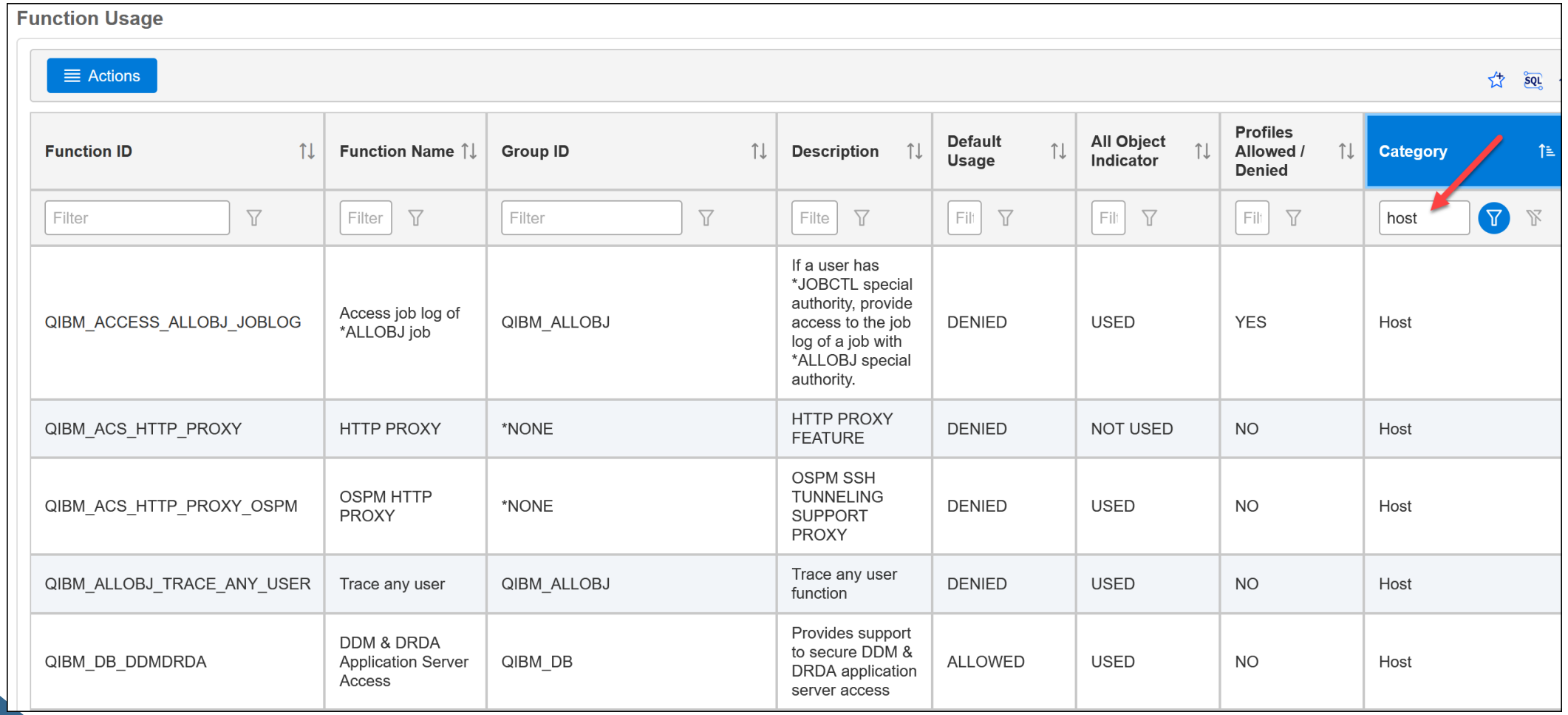


Function Usage

Actions

Function ID	Function Name	Group ID	Description	Default Usage	All Object Indicator	Profiles Allowed / Denied	Category
Filter	Fi	Filter	Filte	Fil	Fil	Fi	client
QIBM_XE1_5250	5250 Display and Printer Emulator	*NONE	Provides support for PC clients to work with the server using a 5250 emulator.	ALLOWED	USED	NO	Client (ACS)
QIBM_XE1_ODBC	ODBC Support	*NONE	Provides access to server data using the ODBC driver.	ALLOWED	USED	NO	Client (ACS)
QIBM_XE1_OLEDB	OLE DB Provider	*NONE	Provides access to server tables, data queues, programs, and commands.	ALLOWED	USED	NO	Client (ACS)
QIBM_XE1_RMTCMD	Remote Command - Command Line	*NONE	Provides support to run commands on a server from the Windows command line	ALLOWED	USED	NO	Client (ACS)

Define Operating System Functions (Host)



Function Usage

Actions

Function ID	Function Name	Group ID	Description	Default Usage	All Object Indicator	Profiles Allowed / Denied	Category
Filter	Filter	Filter	Filte	Fil	Fil	Fil	host
QIBM_ACCESS_ALLOBJ_JOBLOG	Access job log of *ALLOBJ job	QIBM_ALLOBJ	If a user has *JOBCTL special authority, provide access to the job log of a job with *ALLOBJ special authority.	DENIED	USED	YES	Host
QIBM_ACS_HTTP_PROXY	HTTP PROXY	*NONE	HTTP PROXY FEATURE	DENIED	NOT USED	NO	Host
QIBM_ACS_HTTP_PROXY_OSPM	OSPM HTTP PROXY	*NONE	OSPM SSH TUNNELING SUPPORT PROXY	DENIED	USED	NO	Host
QIBM_ALLOBJ_TRACE_ANY_USER	Trace any user	QIBM_ALLOBJ	Trace any user function	DENIED	USED	NO	Host
QIBM_DB_DDMDRDA	DDM & DRDA Application Server Access	QIBM_DB	Provides support to secure DDM & DRDA application server access	ALLOWED	USED	NO	Host

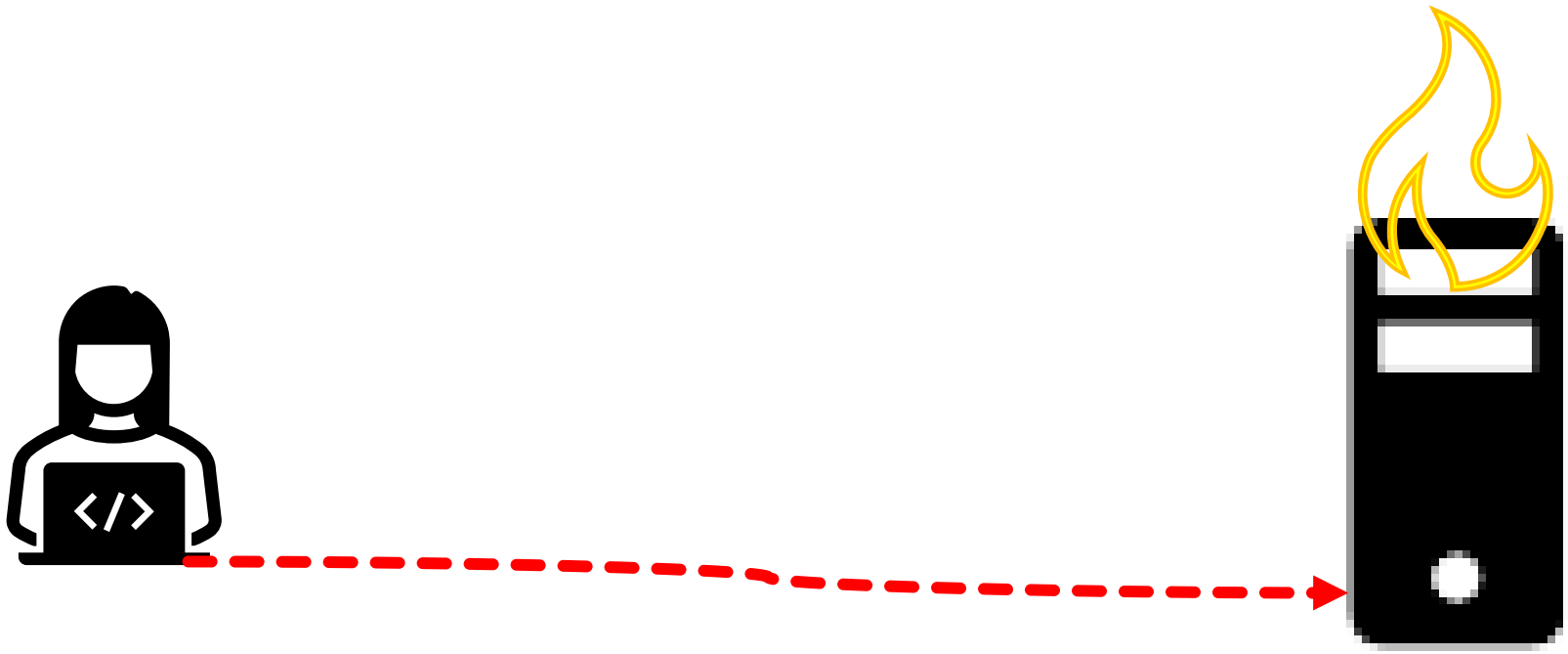
kisco

Services for Function Usage

```
157 -- Function Usage settings for all registered functions (including functions such as Op Nav no longer in use)
158 --
159 SELECT *
160    FROM QSYS2.FUNCTION_INFO
161    ORDER BY FUNCTION_ID;
162 stop;
163 --
164 -- Function Usage info by user
165 --
166 SELECT *
167    FROM QSYS2.FUNCTION_USAGE
168    ORDER BY FUNCTION_ID,
169          USER_NAME;
170 stop;
```

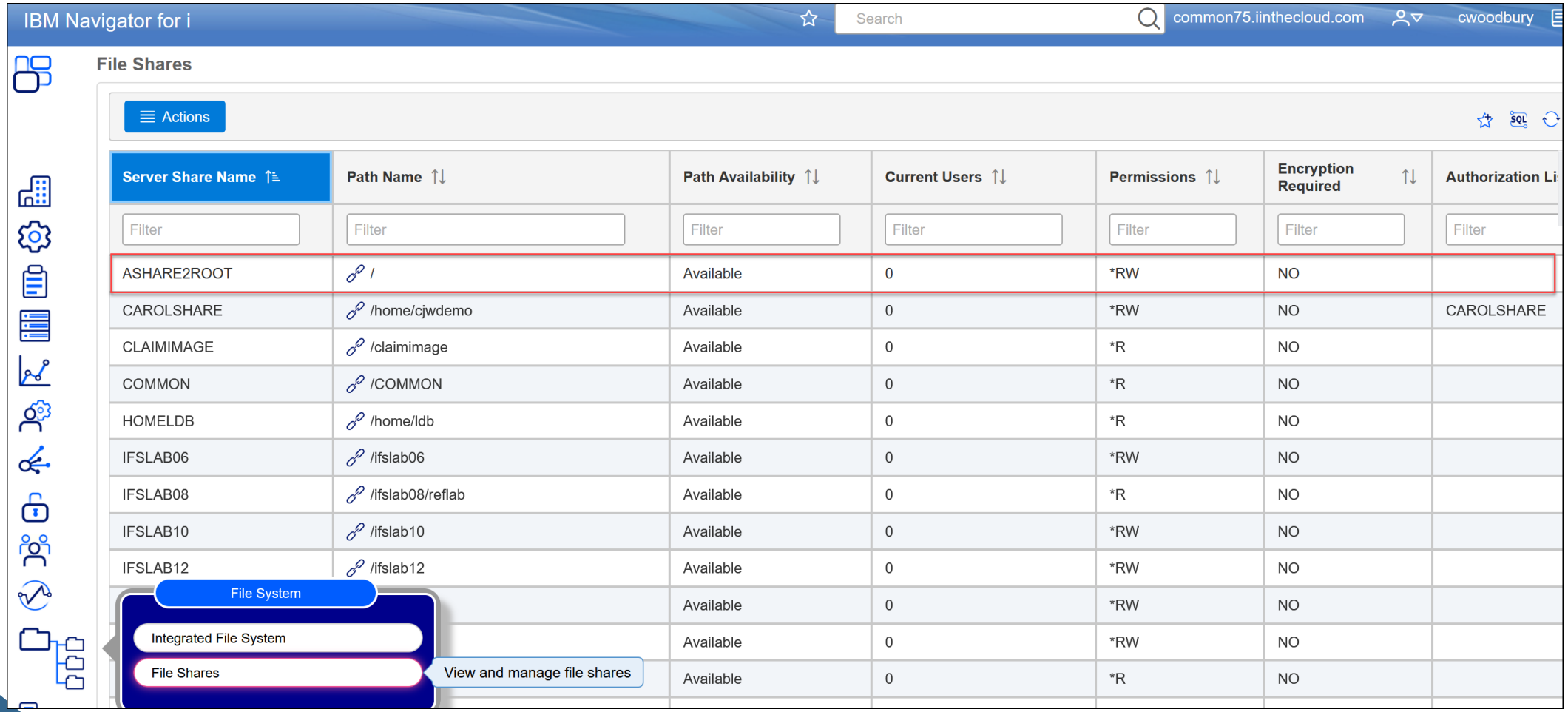
Function ID FUNCTION_ID	User Name USER_NAME	Usage USAGE	User Type USER_TYPE
QIBM_ACCESS_ALLOBJ_JOBLOG	CWOODBURY	ALLOWED	GROUP
QIBM_ACCESS_ALLOBJ_JOBLOG	QPGMR	ALLOWED	GROUP
QIBM_DB_SECADM	DAWN	ALLOWED	USER
QIBM_DB_SECADM	DAWNM	ALLOWED	GROUP
QIBM_DB_SECADM	DAWNMAY	ALLOWED	GROUP
QIBM_DB_SECADM	RCAC_G99	ALLOWED	GROUP
QIBM_DB_SECADM	RMOELLER	ALLOWED	USER

kisco



Evaluate File Shares (Netserver)

File Shares



Worst possible scenario is to have a Read/Write share to root

Using the QSYS2.server_share_info Service

```
93  SELECT server_share_name,
94         path_name,
95         text_description,
96         permissions,
97         share_authorization_list,
98         current_connections,
99         encryption_required
100      FROM qsys2.server_share_info;
101
```

Server Share Name SERVER_SHARE_NAME	Path Name PATH_NAME	Text Description TEXT_DESCRIPTION	Permissions PERMISSIONS	Share Authorization List SHARE_AUTHORIZATION_LIST	Current Connections CURRENT_CONNECTIONS	Encryption Required ENCRYPTION_REQUIRED
LABPX	/LABPX	-	*RW	-	0	NO
WEBSHARE	-	Access for Web print share	-	-	-	NO
WALABRO	/walab	System i Access for Web lab, read only	*R	-	0	NO
WALABRW	/walab	System i Access for Web lab, read only	*RW	-	0	NO
IFSLAB06	/ifslab06	-	*RW	-	0	NO
REFLAB08	/ACSLab	Ref Lab 08	*R	-	0	NO
IFSLAB08	/ifslab08/reflab	Barb share	*R	-	0	NO
IFSLAB12	/ifslab12	-	*RW	-	0	NO
IFSLAB10	/ifslab10	CHRISD	*RW	-	0	NO
IWAAFP	-	Print share for printer Iwaafp	-	-	-	NO
COMMON	/COMMON	Common Dir	*R	-	0	NO
LARRYHOME	/home/ldb	Larrys Home Directory	*R	-	0	NO
HOMELDB	/home/ldb	Larrys Home	*R	-	0	NO
ASHARE2ROOT	/	Sharing root - aka the entire system	*RW	-	0	NO
CAROLSHARE	/home/cjwdemo	Demoing assigning autl to a share	*RW	CAROLSHARE	0	NO

IBM i 7.5 adds the authorization list assigned to the share

kisco

Review Shares

- Determine if shares are in use. If not, delete.
- Review remaining shares to determine if required
  - When initially mapped, ‘Reconnect at sign-on’ was checked
  - Users may have changed jobs and may no longer need access
  - Desktop setup may default to configuring / attaching mapped drives
  - File share access on other platforms should also be reviewed

kisco

Get/Stay Current

Stay Current!

- OS level
  - Many security enhancements – including protocols and cipher suites that may be needed for compliance - aren't available in lower releases.
  - IBM i 7.3 - end of support: September 30, 2023
- Technology Refresh
  - https://www.ibm.com/support/pages/node/1119123
- Access Client Solutions (ACS)
  - Client Access out of support as of April 30, 2019

kisco

PTF Currency

```
160 SELECT *
161   FROM systools.group_ptf_currency
162   ORDER BY ptf_group_level_available - ptf_group_level_installed DESC;
163   stop;
164 stop;
```

PTF_GROUP_CURRENCY	PTF_GROUP_ID	PTF_GROUP_TITLE	PTF Group Level PTF_GROUP_LEVEL_INSTALLED	PTF_GROUP_LEVEL_AVAILABLE	LAST_UPDATED_
JPDATE AVAILABLE	SF99959	SF99959 750 Group Hiper	45	48	2024-02-20
JPDATE AVAILABLE	SF99958	SF99958 750 Group Security	25	27	2024-02-20
JPDATE AVAILABLE	SF99671	SF99671 750 Db2 Web Query for i V2.3.0	8	9	2023-07-19
JPDATE AVAILABLE	SF99676	SF99676 750 High Availability for IBM i	6	7	2024-01-19
JPDATE AVAILABLE	SF99953	SF99953 750 Performance Tools	2	3	2024-01-16
-	SF99669	SF99669 750 Content Manager OnDeman...	6	6	2023-08-25
NSTALLED LEVEL IS CURRENT	SF99677	SF99677 750 750 TCP/IP PTF	4	4	2023-11-27
NSTALLED LEVEL IS CURRENT	SF99750	Current Cumulative PTF Media Document	23306	23306	2023-11-16

Defective PTF Detection

```
166  -- Determine if there are any defective PTFs on the system not already fixed
167  --
168  select *
169   from systools.defective_ptf_currency;
170
```

PARTITION_NAME	HOST_NAME	SERIAL_NUMBER	OS_RELEASE_LEVEL	DEFECTIVE_PTF	APAR_ID	PRODUCT_ID	FIXING_PTF
COMMON1	Common1.Frankeni.com	780EB30	V7R4	SI81255	SE79238	5770SS1	SI82518
COMMON1	Common1.Frankeni.com	780EB30	V7R4	SI80771	SE79143	5770SS1	SI82487
COMMON1	Common1.Frankeni.com	780EB30	V7R4	SI80445	SE79143	5770SS1	SI82487
COMMON1	Common1.Frankeni.com	780EB30	V7R4	MF67678	MA48544	5770999	UNKNOWN

An empty list is a good thing!

kisco

Firmware Currency

```
174 --
175 SELECT * FROM SYSTOOLS.FIRMWARE_CURRENCY;
176 stop;
```

FW_CURRENCY	FW_CURRENTFIXPACK	FW_RELEASE_DATE	FW_MACHINE_TYPE_MODEL	FW_RECOMMENDED_UPDATE	FW_RECOMMENDED_UPGRADE
JPDATE AVAILABLE	VL950_105	2022-07-29	9009-42A	VL950_145	-

Get/Stay Current

- Don’t forget about 3rd party software!
  - Upgrades
  - Patches
- New functionality plus fixes including security

kisco

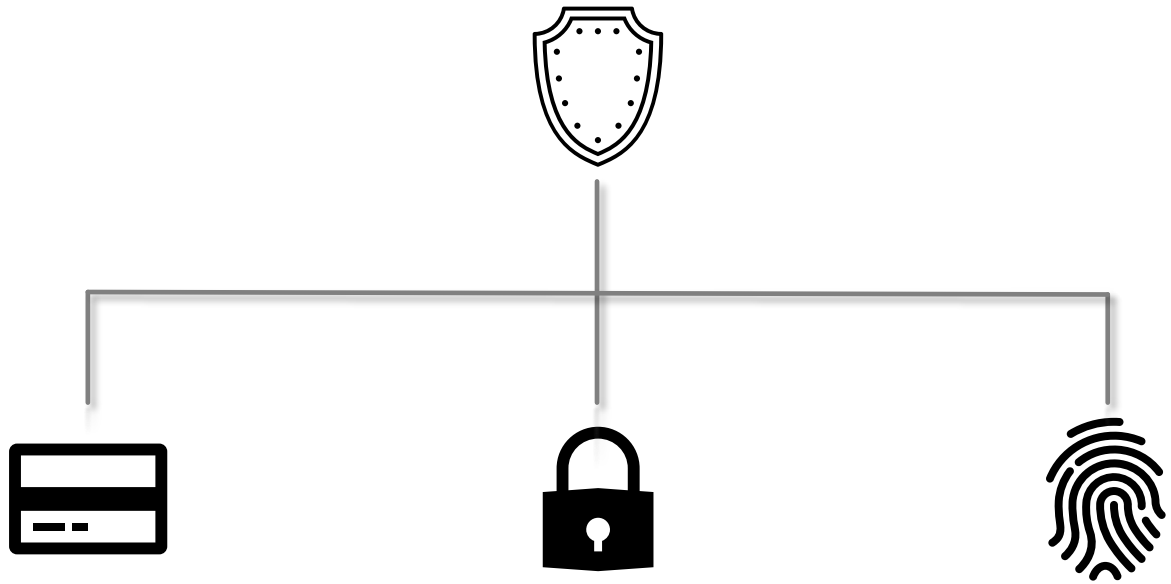
Bonus Task!

Multi-Factor Authentication

kisco

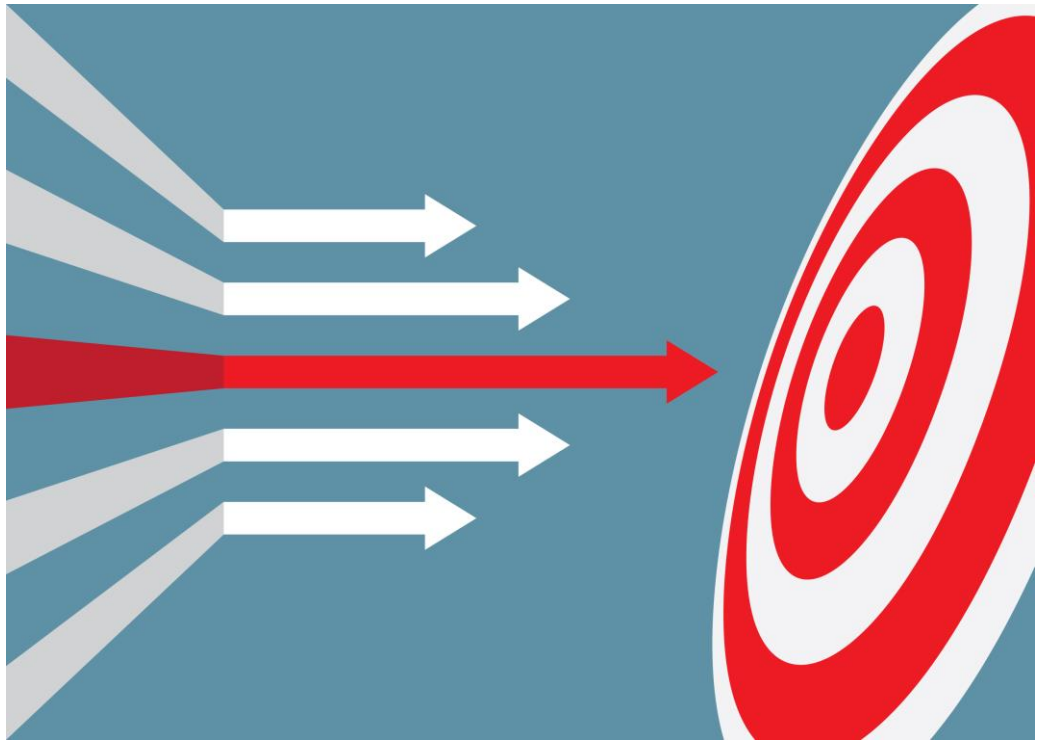
BONUS: Multi-factor Authentication (MFA)

- Use MFA for VPN access *at a minimum*
- Required for internal access by PCI DSS



kisco

What's the Goal of Doing These Tasks … ?



Reduce Risk!

For More Information

From Kisco Systems

Get help at any time with **Kisco Concierge**

Kisco U: https://www.kisco.com/u/index.html

Whitepaper: Securing IBM i: A Dual Responsibility

Books by Carol Woodbury:

IBM i Security Administration and Compliance, 3rd edition, by Carol Woodbury, 2020

Mastering IBM i Security - A Modern Step-by-Step Guide by Carol Woodbury, 2022

Both available from Amazon or MCPress Bookstore

From IBM

IBM i Services Documentation: https://www.ibm.com/support/pages/node/1119123

IBM i Security Reference – PDF:

https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_75/rzarl/sc415302.pdf?view=kc

IBM Tutorials: https://www.ibm.com/support/pages/ibm-i-tutorials-demos-and-sql-examples-0

kisco

General Security Information

Cybersecurity & Infrastructure Security Agency

https://www.cisa.gov/resources-tools/all-resources-tools

NIST

https://www.nist.gov/cyberframework

SANS Organization

https://www.sans.org/

Newsletters

https://www.secureworld.io/

https://www.securityweek.com/

https://www.bankinfosecurity.com/

https://www.darkreading.com/

https://krebsonsecurity.com/

kisco

Questions?

Contact: justin@kisco.com
steve@kisco.com