What's New in IBM i Security

Carol Woodbury CISSP, CRISC
IBM CHAMPION
IBM i Security SME and Senior Advisor, Kisco Systems
carol@kisco.com

1

IBM's Commitment to 'Secure by Design'

https://www.ibm.com/support/pages/ibm-security-and-privacy-design

2

Secure by Design

- Set system objects to *PUBLIC(*USE) that weren't
- Must have some authority to objects in /home to be displayed in list
- SQL views now require the same authorities as the corresponding CL command
- Some network configuration interfaces now require *IOSYSCFG or have authority to the new QIBM_IOSYSCFG_VIEW function.

Webinar: https://www.kisco.com/ibm-i-security-a-dual-responsibility.html

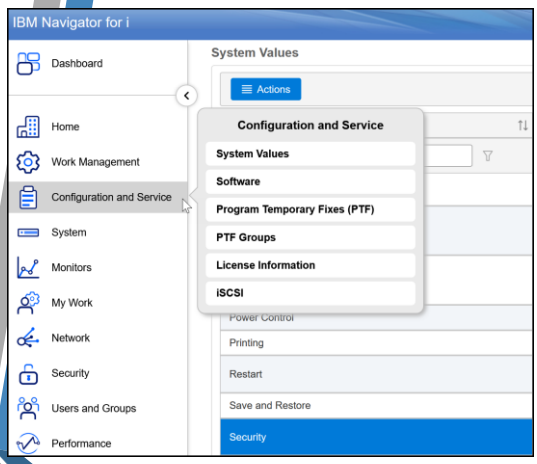
Whitepaper: Securing IBM i: A Dual Responsibility

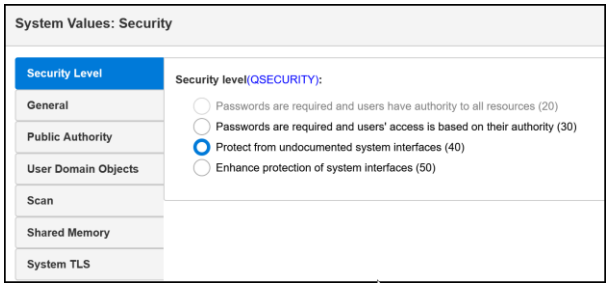
3

Security Level and Auditing

4

QSECURITY – Security Level





5

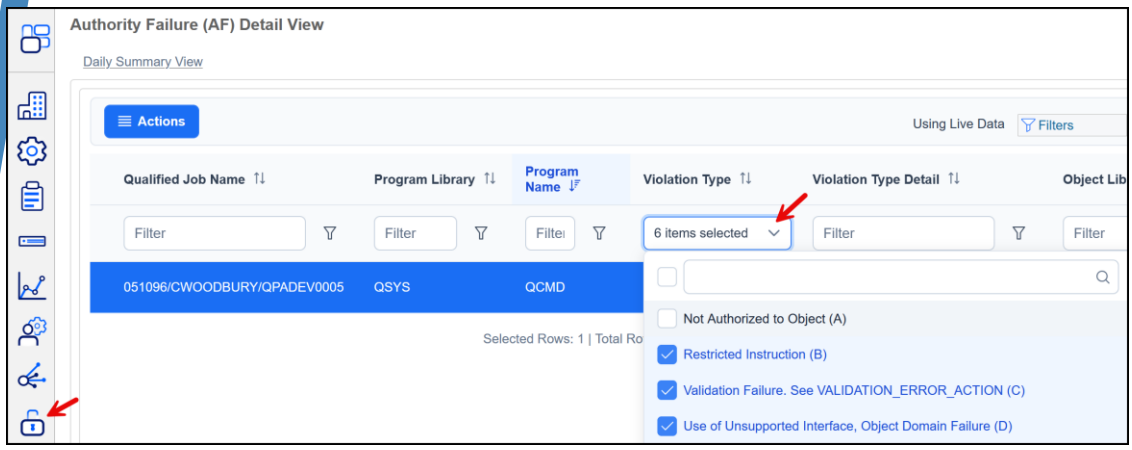
QSECURITY level 20

7.5

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

6

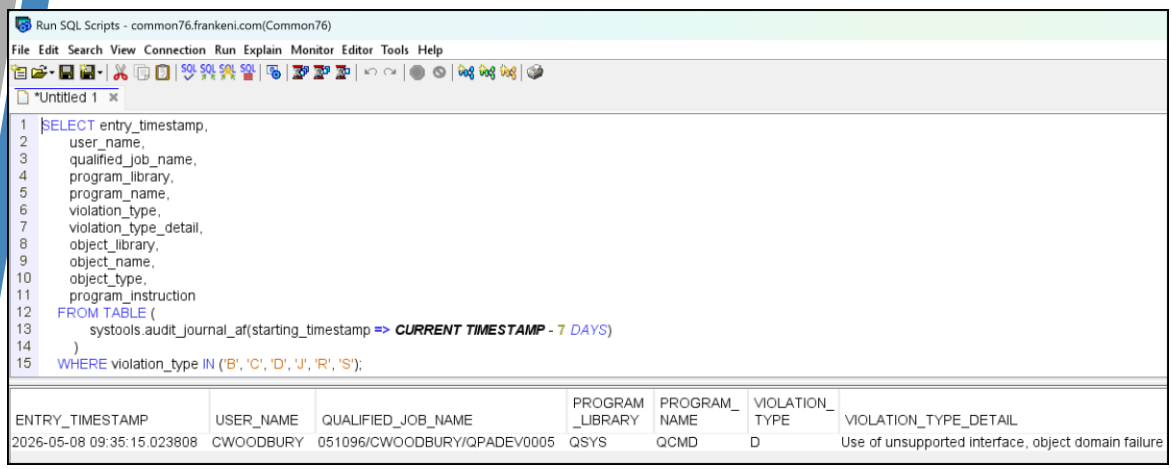
Audit Entries in Navigator for i – Detailed View



kisco

7

Using AF Audit Helper Function to Move to Level 40



QAUDCTL must include *AUDLVL
QAUDLVL must include *AUTFAIL and *PGMFAIL

kisco

8

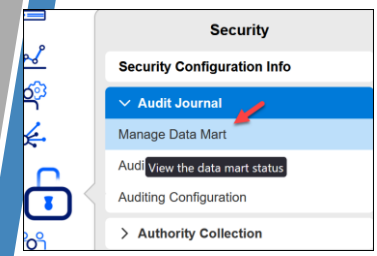
Audit Journal Entry SQL Table Functions

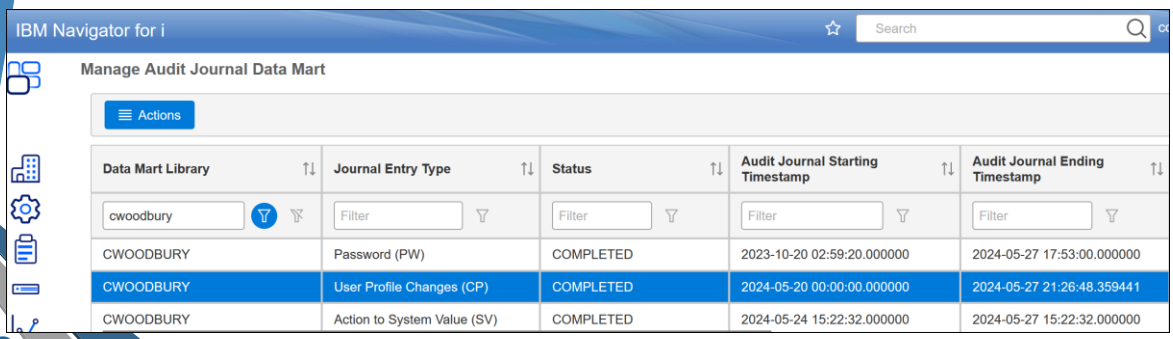
- Original helper functions included:
  - AF – Authority Failure (SYSTOOLS.AUDIT_JOURNAL_AF)
  - CA – Changes to Authority (SYSTOOLS. AUDIT_JOURNAL_CA)
  - OW – Ownership Changes (SYSTOOLS. AUDIT_JOURNAL_OW)
  - PW – Password (SYSTOOLS. AUDIT_JOURNAL_PW)
- Available beginning in V7R3 TR10 and V7R4 TR4
- Now, most audit journal entry types are available:
  - https://www.ibm.com/docs/en/i/7.6?topic=services-audit-journal-entry
  - https://www.ibm.com/support/pages/node/6442047

9

Audit Journal Data Marts

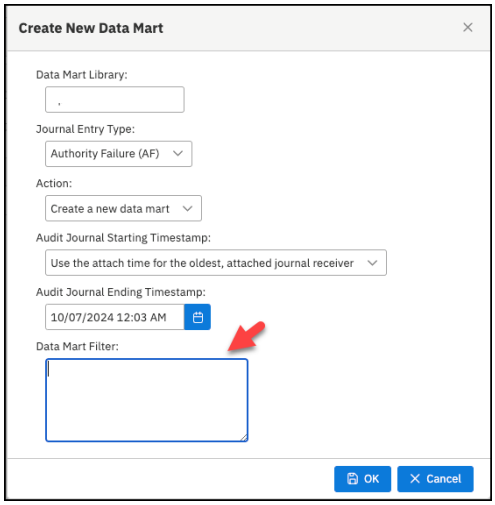
IBM i 7.5 TR4
IBM i 7.4 TR10





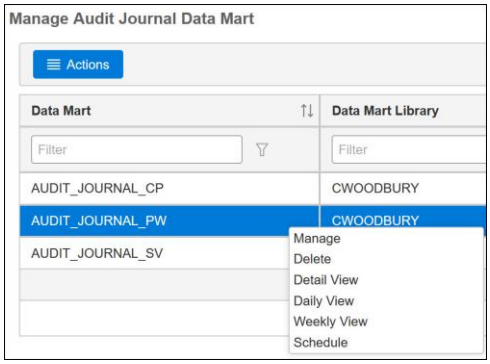
10

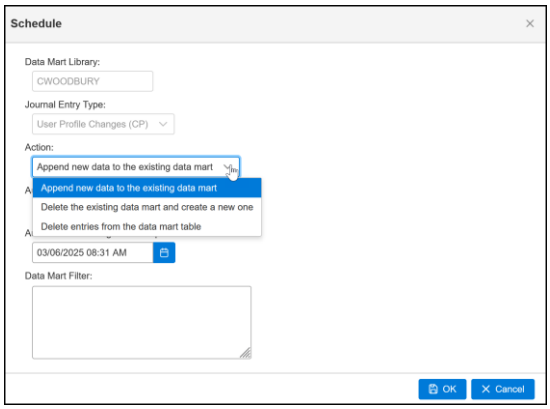
Create a New Audit Journal Data Mart



11

Data Mart Options





12

QSYS2.manage_audit_journal_data_mart

Create the data mart … results in the creation of a file audit_journal_CP in library YOUR_LIB

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART(
  JOURNAL_ENTRY_TYPE => 'CP',
  DATA_MART_LIBRARY  => 'YOUR_LIB',
  STARTING_TIMESTAMP => '*FIRST',
  ENDING_TIMESTAMP   => DEFAULT,
  DATA_MART_ACTION   => 'CREATE'
);
```

Add entries

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART (
  JOURNAL_ENTRY_TYPE => 'CP',
  DATA_MART_LIBRARY  => 'YOUR_LIB',
  STARTING_TIMESTAMP => '*CONTINUE',
  ENDING_TIMESTAMP   => NULL,
  DATA_MART_ACTION   => 'ADD'
);
```

kisco

13

Data_Mart_Filter parm

IBM i 7.5 TR5
IBM i 7.4 TR11

```
CALL QSYS2.MANAGE_AUDIT_JOURNAL_DATA_MART(JOURNAL_ENTRY_TYPE => 'DO',
        DATA_MART_LIBRARY => 'AUDIT_INFO',
        STARTING_TIMESTAMP => *FIRST,
        ENDING_TIMESTAMP => CURRENT TIMESTAMP,
        DATA_MART_FILTER => 'OBJECT_TYPE = ''*USRPRF'' ');
```

kisco

14

Passwords

15

Password Level (QPWDLVL)

7.5

System value	
0 / 1 are the same	Default until IBM i 7.6 Character set: A-Z, 0-9, $, @, # and _ Maximum length: 10 LanMan password not stored at ANY level
2	Character set: Upper / lower case, all punctuation and special characters, numbers and spaces Maximum length: 128 Encrypts with old and new algorithms to accommodate both levels 0/1, 2/3 and 4 Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed
3	Same as level 2, gets rid of old encrypted password Level 4 password generated and retained Default for new installs as of IBM i 7.6
4 (new in IBM i 7.5)	Stronger algorithm to store password hash. Only version stored is the one that works at level 4* *Note: Requires ACS 1.1.9.0 or higher!

16

New Password System Value Defaults

7.6

```
                          Display System Value

System value . . . . . :   QPWDLVL
Description  . . . . . :   Password level


Password level . . . . :   3
```

```
                          Display System Value

System value . . . . . :   QPWDRULES
Description  . . . . . :   Password rules


Password                                    Password
rules                                       rules
*ALLCRTCHG
*LMTPRFNAME
*MINLEN15
*REQANY3
```

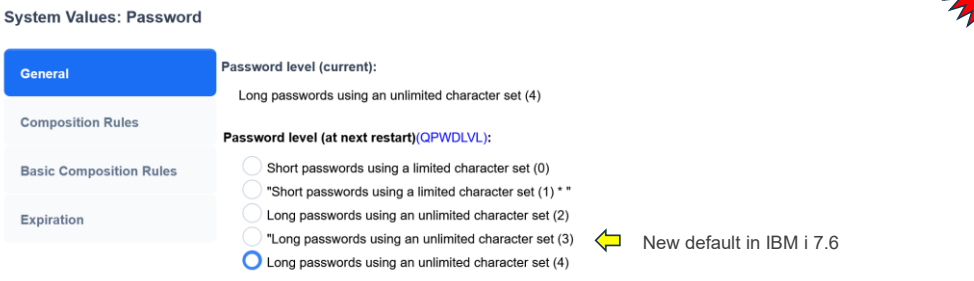
NEW INSTALLS ONLY !!!

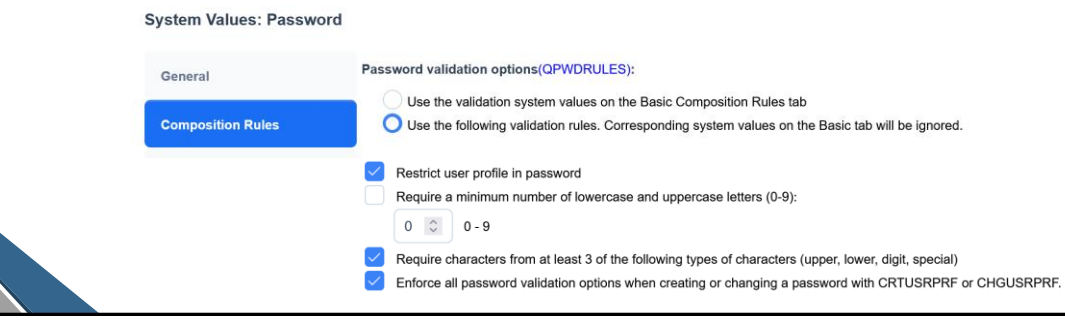
kisco

17

New Defaults in IBM i 7.6

7.6





kisco

18

Password Hashes Stored at Each Level

Password hashes generated at QPWDLVL 0/1	Password hashes generated at QPWDLVL 2	Password hashes generated at QPWDLVL 3	Password hash generated at QPWDLVL 4
All uppercase All lowercase Regardless of what the user types (Car0L) the password is folded: CAR0L car0l	> Password no longer folded for authentication Used for authentication: Mixed case – Level 2/3 Hashes generated when password is changed: - Mixed case – Level 2/3 - All uppercase – Lvl 0/1 - All lowercase – Lvl 0/1 - Mixed case – Level 4	Used for authentication: Mixed case – Level 2/3 Hashes generated when password is changed: - Mixed case – Level 2/3 - Mixed case - Level 4	Level 4 version only

Move from 0/1 to 2, test then move to 3 (or 4)
Cannot move directly from 0/1 to 4
Cannot move from 4 to 0/1
All changes require an IPL

19

Same Message Issued for Incorrect User or Password

7.5

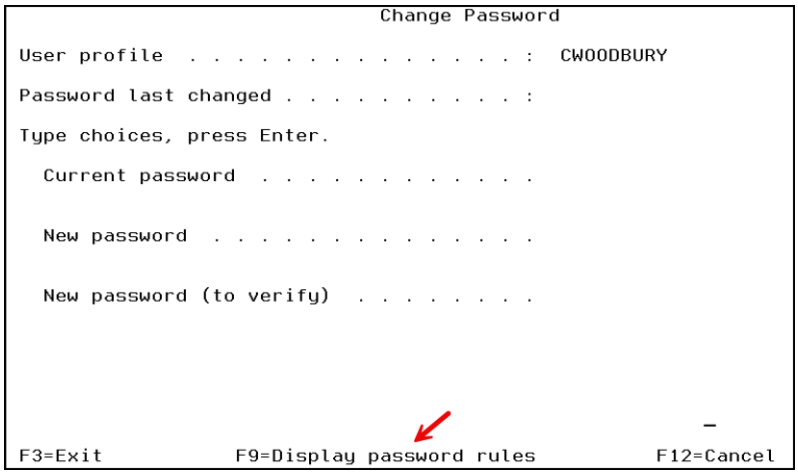
```
                              Sign On
                                          System  . . . . . :   DXREX75
                                          Subsystem . . . . :   QINTER
                                          Display . . . . . :   QPADEV0003

          User  . . . . . . . . . . . . .   CAROL
          Password  . . . . . . . . . . .

          Program/procedure . . . . . . .   __________
          Menu  . . . . . . . . . . . . .   __________
          Current library . . . . . . . .   __________

CPF1120 - User CAROL does not exist or password not correct for user profile.
MA    A                                                          06/053
```

The same message will be issued for both incorrect User or incorrect Password

20

Press F9 to View the Rules!

7.5



21

User Profiles

23

Create User Profile (CRTUSRPRF) – 1 (New default)

7.5

```
                    Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . .   newprofile     Name
User password  . . . . . .   *NONE
_____
Set password to expired  . . . .   *yes          *NO, *YES
Status . . . . . .   *ENABLED      *ENABLED, *DISABLED
User class . . . . . .   *USER       *USER, *SYSOPR, *PGMR...
Assistance level . . . . . .   *SYSVAL     *SYSVAL, *BASIC, *INTERMED...
Current library  . . . . . .   *CRTDFT     Name, *CRTDFT
Initial program to call  . . . .   *NONE       Name, *NONE
  Library  . . . . . .   __________   Name, *LIBL, *CURLIB
Initial menu . . . . . .   MAIN         Name, *SIGNOFF
  Library  . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Limit capabilities . . . . . .   *NO         *NO, *PARTIAL, *YES
Text 'description' . . . . . .   Make this meaningful!!!_
_____
                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Additional parameters   F12=Cancel
F13=How to use this display        F24=More keys
```

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

24

24

Create User Profile – 2 (new Parm)

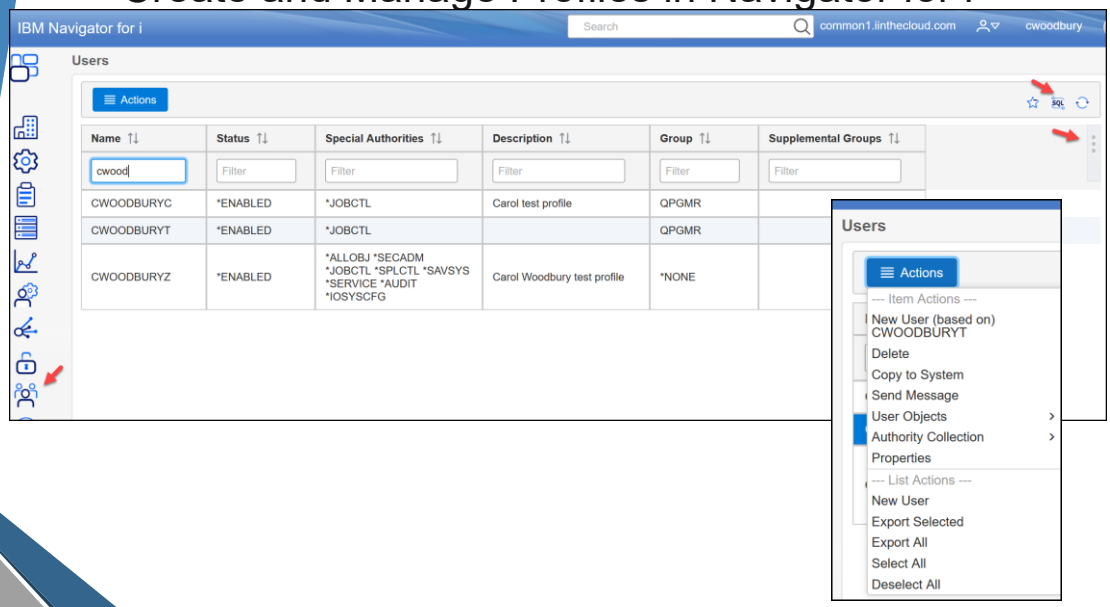
7.5

```
                    Create User Profile (CRTUSRPRF)

Type choices, press Enter.


                          Additional Parameters

Special authority  . . . . . .   *USRCLS      *USRCLS, *NONE, *ALLOBJ...
              + for more values
Special environment  . . . . .   *SYSVAL      *SYSVAL, *NONE, *S36
Display sign-on information  . .   *SYSVAL      *SYSVAL, *NO, *YES
Password expiration interval . .   *nomax      1-366, *SYSVAL, *NOMAX
Block password change  . . . . .   *SYSVAL      1-99, *SYSVAL, *NONE
Local password management  . . .   *YES         *YES, *NO
Maximum sign-on attempts . . . .   *SYSVAL      1-25, *SYSVAL
Limit device sessions  . . . . .   *SYSVAL      *SYSVAL, *YES, *NO, 0, 1...
Keyboard buffering . . . . . .   *SYSVAL      *SYSVAL, *NO, *TYPEAHEAD...
Maximum allowed storage large  .   *NOMAX
Maximum allowed storage  . . . .   *NOMAX       Kilobytes, *NOMAX
Highest schedule priority  . . .   3           0-9
                                                                  More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

25

25

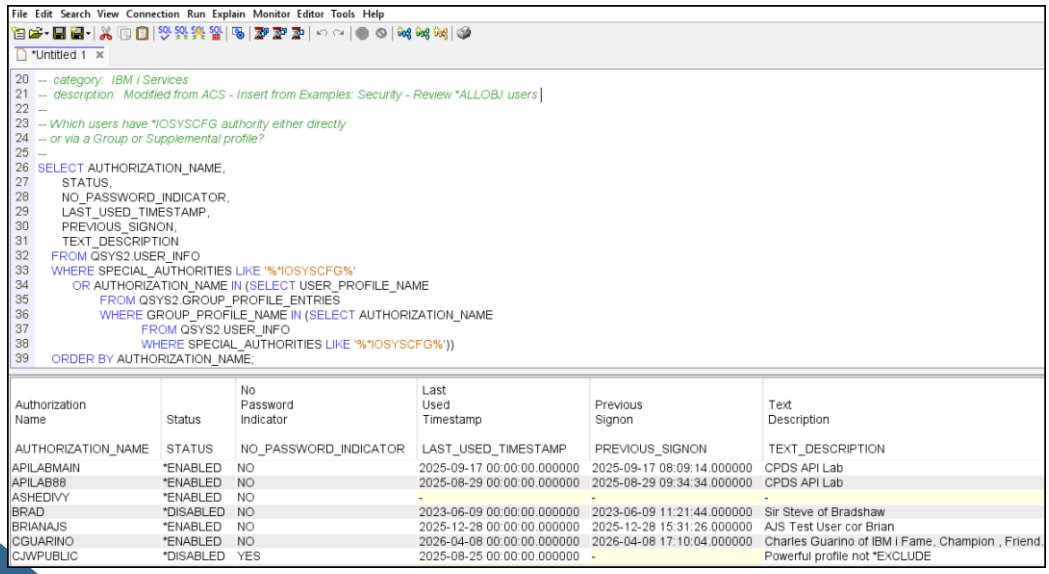
Create and Manage Profiles in Navigator for i



kisco

26

Find Profiles with *IOSYSCFG using qsys2.user_info



kisco

27

IBM i 7.6 Memo to Users (MTU) - *IOSYSCFG Expanded

7.6

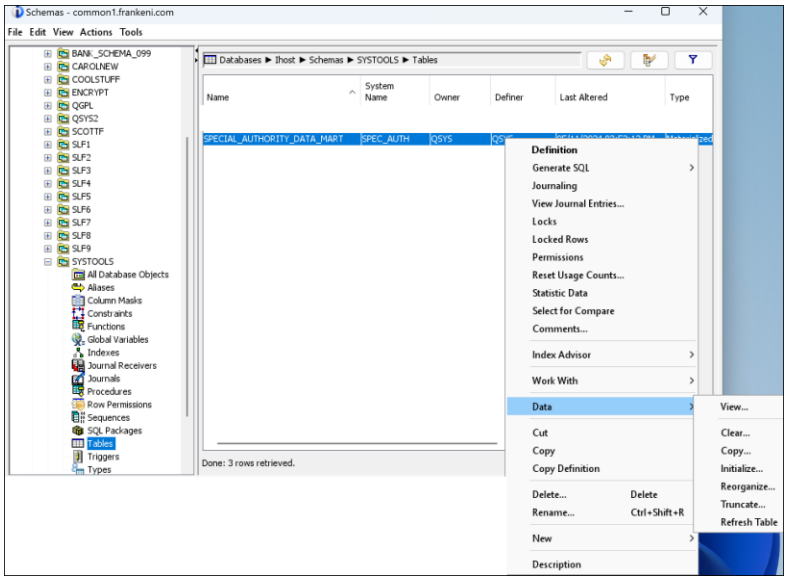
- Command and API Authority Changes (47)
- Some system values and network attributes require *IOSYSCFG or QIBM_IOSYSCFG_VIEW function usage to view or retrieve data (8)
- Network Command and API Authority Changes (27)
- CHGTELNA Command Authority Changes
- QTVRTVTELA API Authority Changes
- Authority requirements change for NetServer shares
- Authority change for tape commands and APIs (17)
- SQL services changed to require *IOSYSCFG or QIBM_IOSYSCFG_VIEW (14)
- Authority changes for Db2 Mirror SQL services (16)
- SQL CREATE ALIAS statement authority change

- IBM i 7.6 Memo to Users : https://www.ibm.com/docs/en/ssw_ibm_i_76/pdf/rzaq9.pdf

kisco

28

SYSTOOLS.Special_Authority_Data_Mart



IBM i 7.5 TR4
IBM i 7.4 TR10

kisco

29

Review Who Has *IOSYSCFG including the Source

IBM i 7.5 TR4
IBM i 7.4 TR10

```
42  -- Who has *IOSYSCFG special authority and from what source(s) ? (Using the Special authority data mart)
43  --
44  SELECT user_name,
45       authority_source,
46       group_profile_name,
47       status,
48       text_description,
49       last_used_date
50    FROM systools.special_authority_data_mart
51    WHERE special_authority = '*IOSYSCFG'
52    ORDER BY user_name;
```

Authorization Name	Authority Source	Group Profile Name	Status	Text Description	Last Used Date
USER_NAME	AUTHORITY_SOURCE	GROUP_PROFILE_NAME	STATUS	TEXT_DESCRIPTION	LAST_USED_DATE
TIMCLARK	USER PROFILE	-	*DISABLED	-	2024-04-29
TIMMR	USER PROFILE	-	*ENABLED	Tim M Rowe - IBM Presentor extrordinaire	2026-01-13
TIMMR	GROUP PROFILE	SUPERUSER	*ENABLED	Tim M Rowe - IBM Presentor extrordinaire	2026-01-13

kisco

32

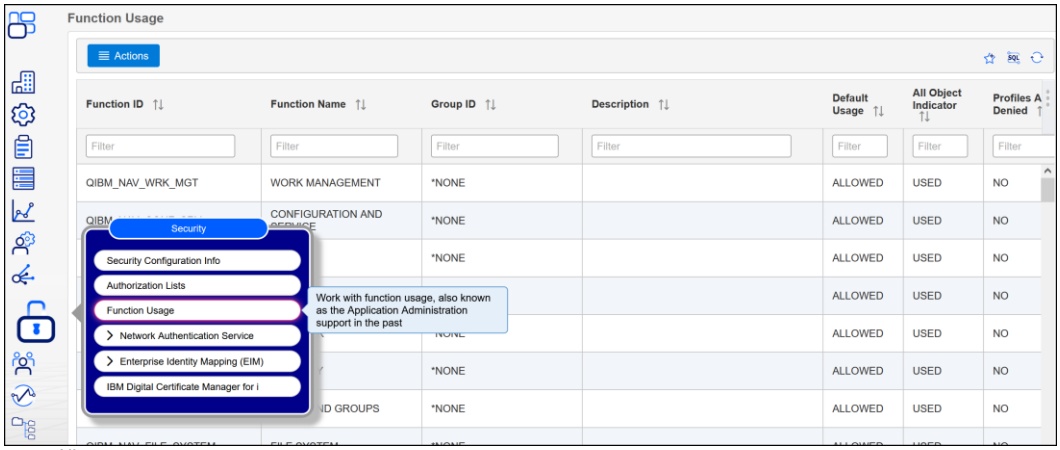
7.6

Increased Use of Function Usage

kisco

33

Function Usage (previously Application Administration)

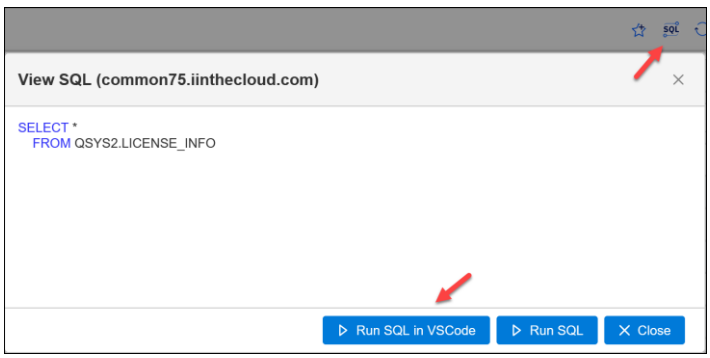


Allows you to:

- customize which users see:
  - Navigator for i features
  - ACS features
- control functions when there's no object to secure
  - e.g., access joblog of an *ALLOBJ user, on/off controls for FTP, ODBC and DDM

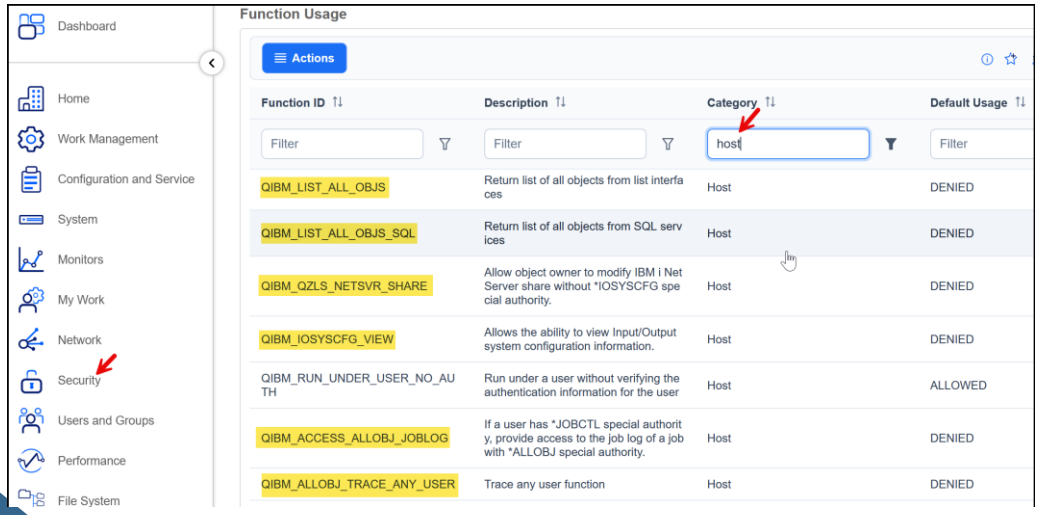
34

It's Not Just ACS Anymore!



35

Function Usage in Navigator for i



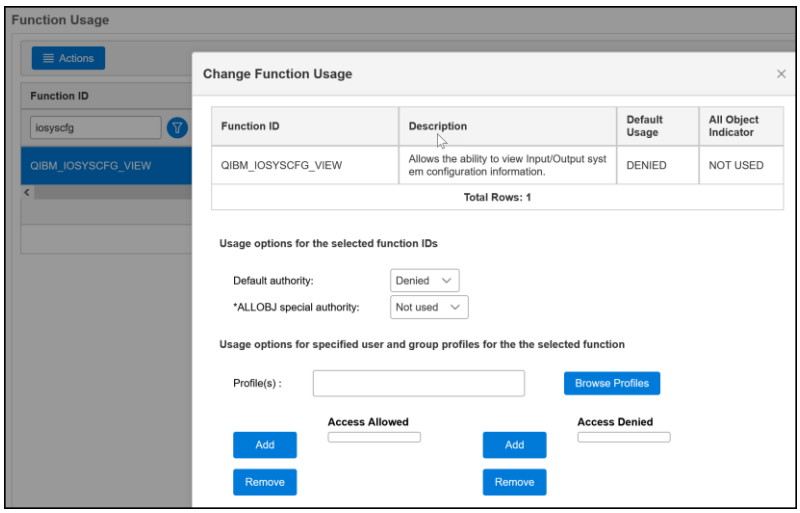
For the full list of IBM-supplied function IDs, see IBM i Security Reference, Appendix H

36

36

QIBM_IOSYSCFG_VIEW function

7.6

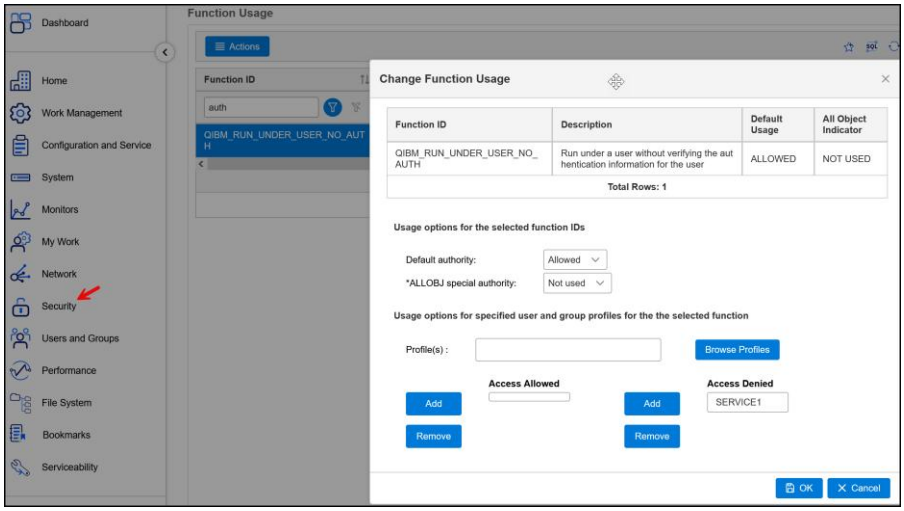


Provides the ability to view network config information without granting full *IOSYSCFG access

37

QIBM_RUN_UNDER_NO_AUTH

7.6



Allows you to protect 'powerful' profiles from being exploited

40

New User Audit Value

7.6

- *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 in 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 – not in QAUDLVL
    - Produces a GR entry

41

Other New Things

New IBM-Supplied User Profiles

7.6

- QPGMR_NC
  - Neither QPGMR nor QPGMR_NC will have *SAVSYS!
- QRCL (Remote code load server profile)
- QRSC (Remote code load profile)
- QSECOFR_NC
- QSYSOPR_NC
- QUSER_NC

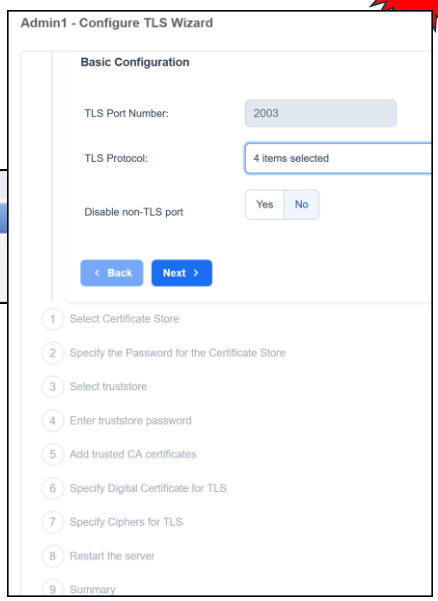
➡ Note: Leave these as Operating System profiles!!!

- Don't make them object owners
- Don't use them as a group profile!

Emphasis on Using Secure Ports

7.6

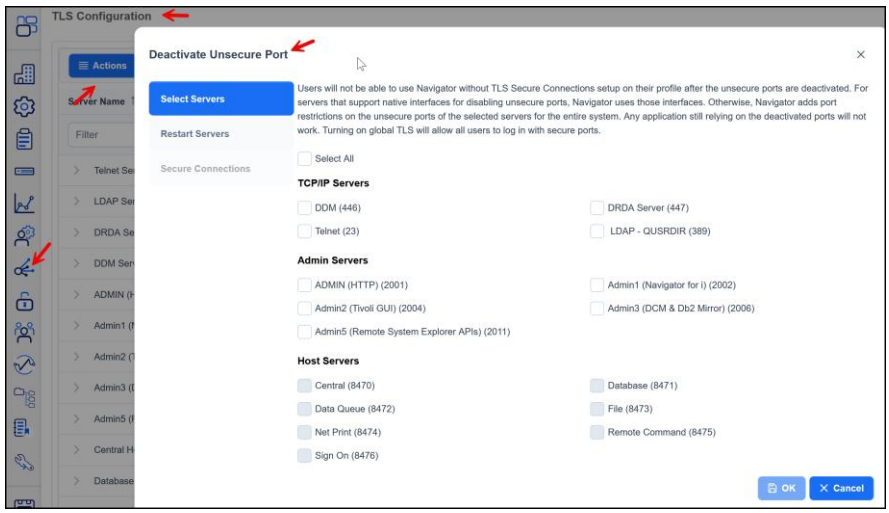
IBM i 7.5 TR5
IBM i 7.4 TR11



46

Easy to Turn off Unsecure Ports!

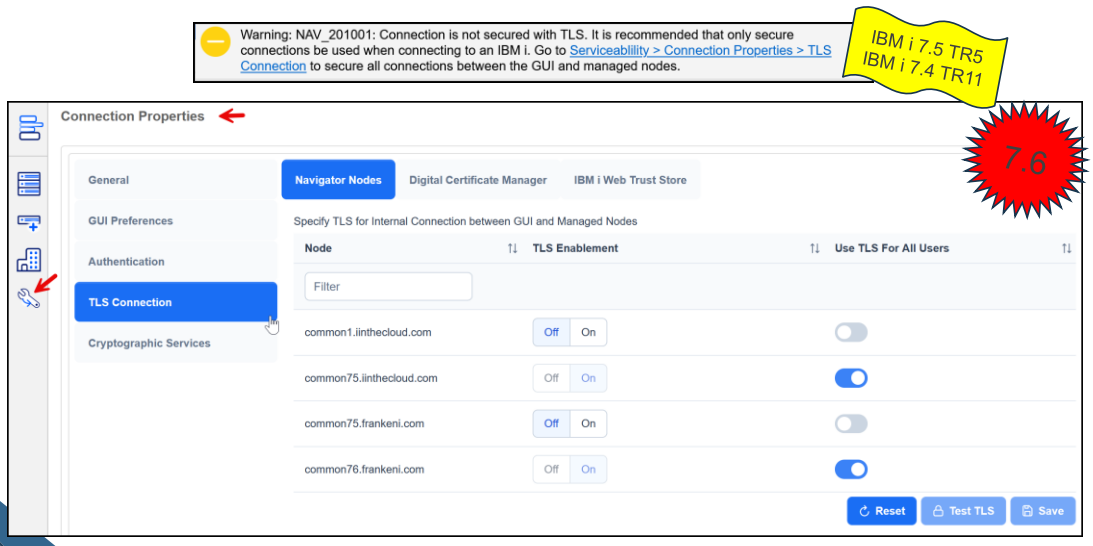
7.6



Network->Servers->TLS Configuration

47

Emphasis on Using Encrypted (TLS) Sessions



Dashboard view -> Serviceability -> Connection Properties

48

Clean up !

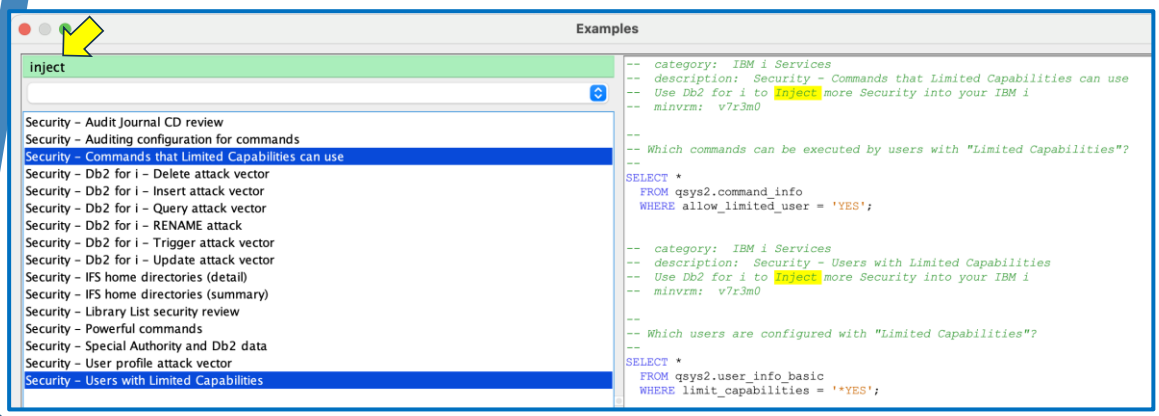
7.6

IBM i 7.6 removed the following no longer in use:

- User profiles
  - QMGTC, QIBMHELP, and QPM400
- Protocols
  - PPP, QoS, L2TP
- Servers
  - BOOTP, DHCP, DNS, MGTC, QOS, and RouteD

49

New Security-Focused Run SQL – Insert Examples



39 SQL statements available as of ACS 1.1.9.12!!!

50

The Latest ACS Addresses CVEs (only)

Version = 1.1.9.13
Build date = May 2026
ESS Level = LCD8-2010-42

********** ATTENTION **********

This update includes security fixes for the following CVEs:
CVE-2026-41409
CVE-2026-41635
CVE-2026-7770

IBM i Access Client Solutions is vulnerable to remote code execution when configured to listen for requests from IBM i Navigator.

********** ATTENTION **********

51

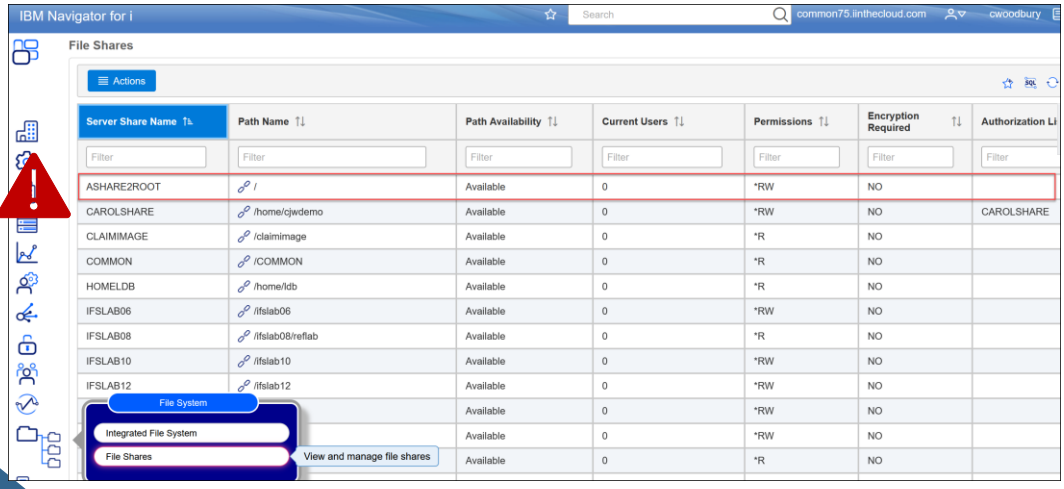
Protecting the System from Malware

52

File Shares !!!

53

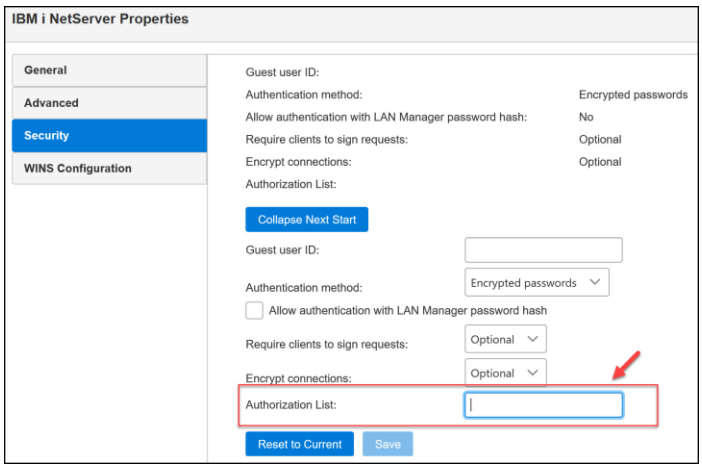
File Shares



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

Controlling Access to NetServer with an *AUTL

7.5



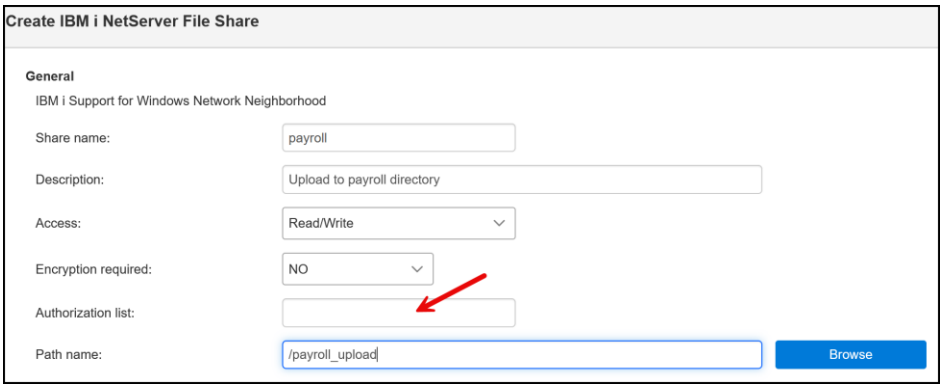
Suggested approach:
- Set *PUBLIC to *EXCLUDE
- Only authorize users who have a business need to map a drive

Remember:
*ALLOBJ provides access!!!

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

Secure Individual Shares with an *AUTL

7.5



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

56

VP Audit Journal Entry

7.5

- 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

57

Who's Using a File Share?

7.6

Answer:

- Add *NETSMBSVR to QAUDLVL
- Generates a **VP** audit entry documenting the use of a file share – including the name of the share!!!

```
303 --
304 -- description: New in IBM i 7.6!
305 --              Add *NETSMBSVR to QAUDLVL and look at the VP audit journal entries to see which shares are in use!
306 --
307 SELECT entry_timestamp,
308        audit_user_name,
309        share_name,
310        entry_type_detail,
311        share_authorization_list
312     FROM TABLE (
313            systools.audit_journal_vp(starting_timestamp => CURRENT TIMESTAMP - 7 DAYS)
314         );
315 stop;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	SHARE_NAME	ENTRY_TYPE_DETAIL	SHARE_AUTHORIZATION_LIST
2025-04-02 10:47:52.333616	CJW	*SERVER	Server or share connection established	-
2025-04-02 10:47:52.693216	CJW	ROOT	Server or share connection established	-
2025-04-02 11:20:12.253872	CJW	ROOT	Server or share connection ended	-
2025-04-02 11:20:12.337952	CJW	*SERVER	Server or share connection ended	-

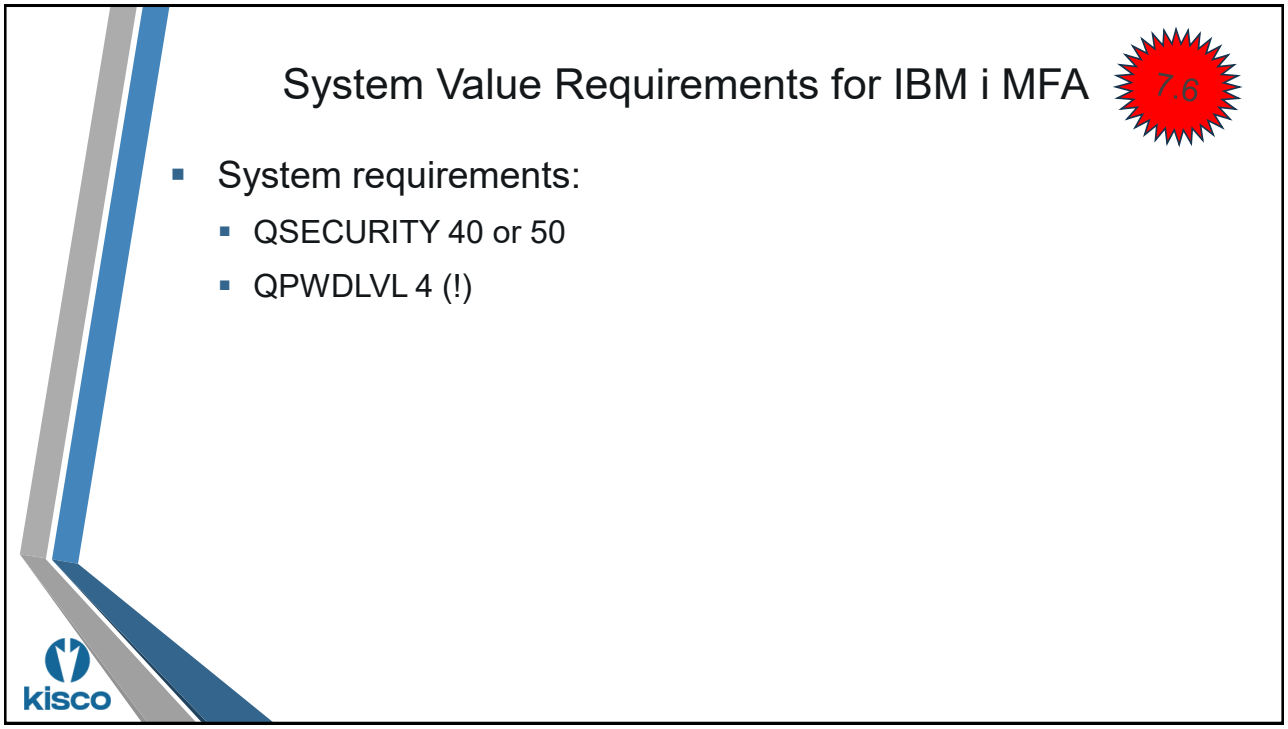
Finding Users of File Shares – IBM i 7.4 and 7.5

Configure Authority Collection on the path being shared:
- CHGAUTCOL OBJ('/home/testnav') AUTCOLVAL(*OBJINF)
- STRAUTCOL TYPE(*OBJAUTCOL)

```
272 -- To determine who's using a file share in IBM i 7.4 and 7.5, configure Authority Collection on the object being shared
273 -- This enhanced/simplified Authority Collection view added in IBM i 7.6 and IBM i 7.5 TR6
274 --
275 cl:CHGAUTCOL OBJ('/HOME/TESTNAV/') AUTCOLVAL(*OBJINF);
276 CL:STRAUTCOL TYPE(*OBJAUTCOL);
277 SELECT user_name, check_timestamp, path_name,
278   detailed_required_authority, detailed_current_authority
279   FROM qsys2.authority_collection_ifs
280   WHERE job_name LIKE 'QZLSFILE%' AND UPPER(path_name) LIKE '/HOME/TESTNAV/%';
281
282 stop;
```

IBM i 7.6
IBM i 7.5 TR6

61



62

Step 1: Enable the System for IBM i MFA

7.6

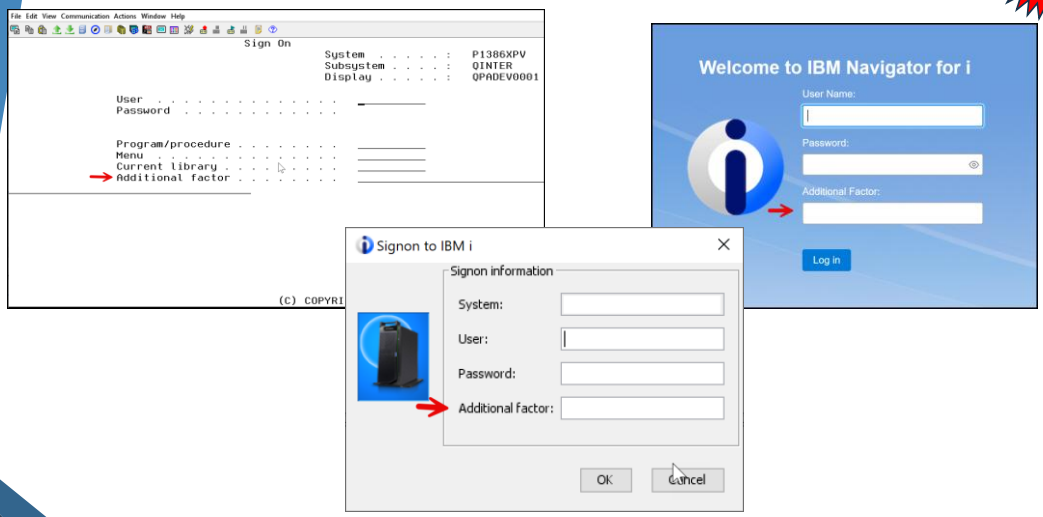
```
                    Change Security Attributes (CHGSECA)

Type choices, press Enter.

User ID number . . . . . .   8490_____     101-4294967294, *SAME
Group ID number  . . . . . .  787          101-4294967294, *SAME
Additional sign-on factor  . . .  *enabled_  *SAME, *ENABLED, *DISABLED
```

Note: this is a security attribute, NOT a system value!

63

Signon Displays after IPL

7.6

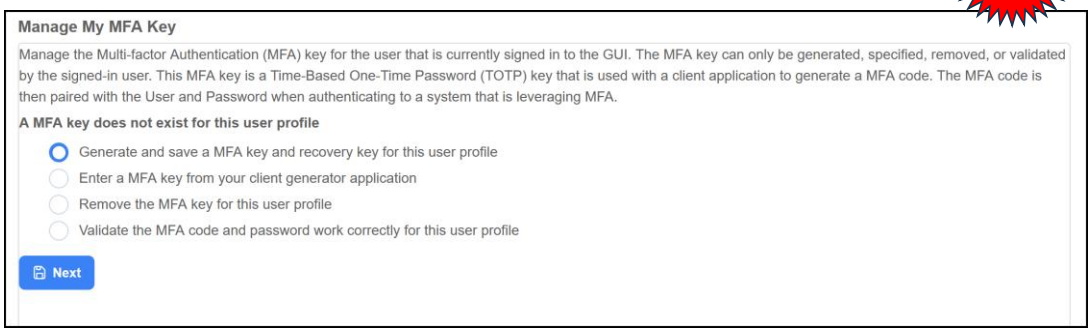


Additional Factor field added to all sign on displays once system is enabled for MFA and IPLed

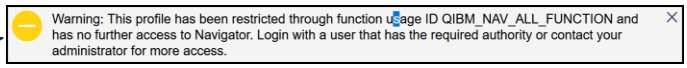
64

Step 2: User Enrollment

7.6



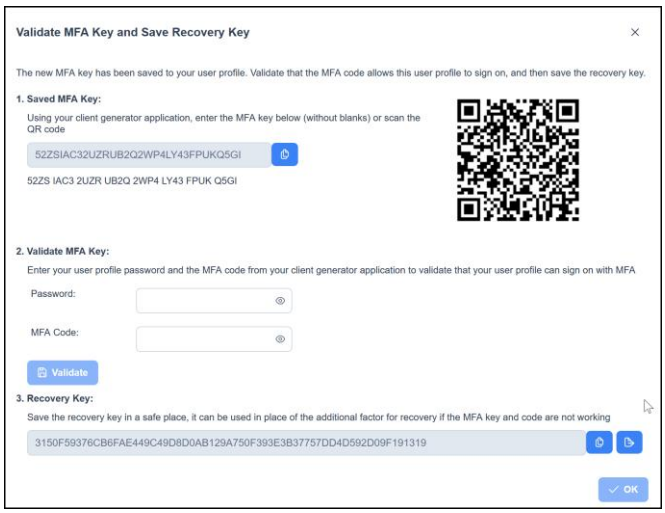
What users not authorized to Navigator for i will see



65

Scan the QR code and Verify

7.6



Use Okta, DUO, Microsoft Authenticator, etc

66

Step 3: Modify the User's Profile

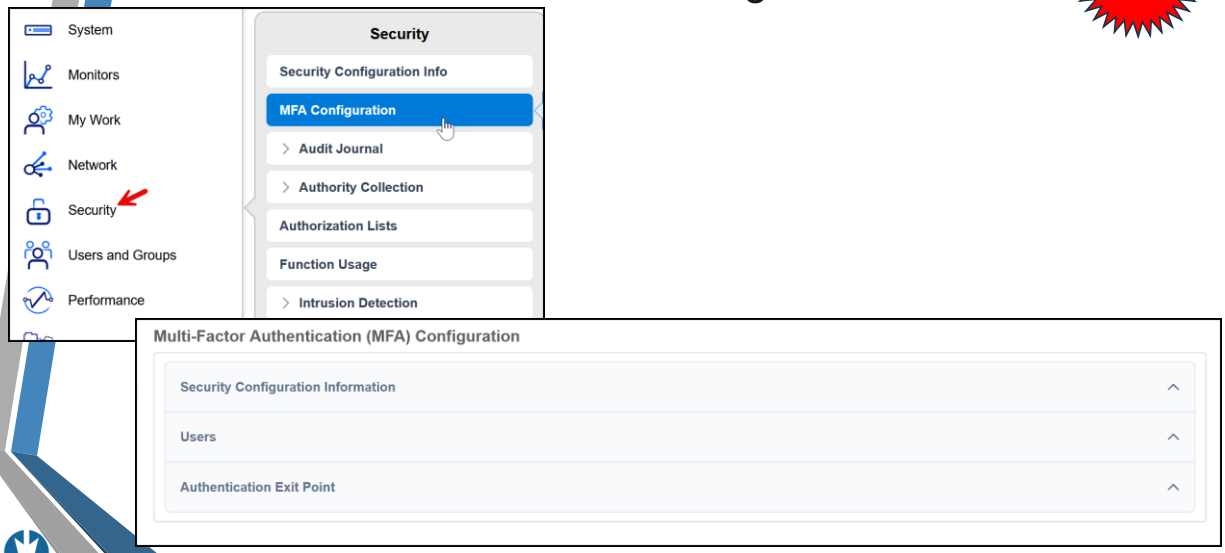
7.6

```
                    Change User Profile (CHGUSRPRF)

Type choices, press Enter.


                              Additional Parameters

Special authority  . . . . . .   *NONE       *SAME, *USRCLS, *NONE...
              + for more values
Special environment  . . . . . .  *SYSVAL     *SAME, *SYSVAL, *NONE, *S36
Display sign-on information  . .  *SYSVAL     *SAME, *NO, *YES, *SYSVAL
Password expiration interval . .  *SYSVAL     1-366, *SAME, *SYSVAL, *NOMAX
Block password change  . . . . .  *SYSVAL     1-99, *SAME, *SYSVAL, *NONE
Local password management  . . .  *YES        *SAME, *YES, *NO
Authentication methods . . . . .  *totp
                                   60
TOTP optional interval . . . . .                1-720, *SAME, *NONE
Maximum sign-on attempts . . . .  *SYSVAL     1-25, *SAME, *SYSVAL
```

IBM i MFA will now be required for this profile

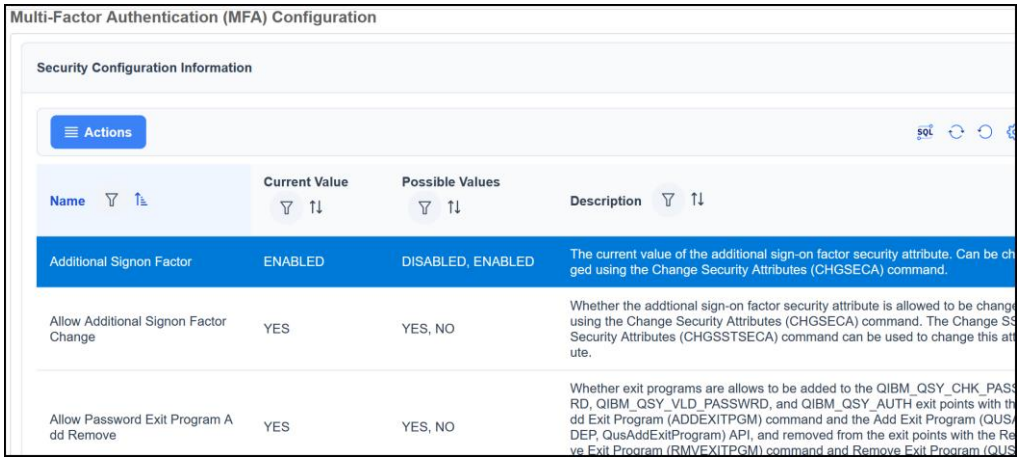
Instead, Just Use Navigator for i ☺

7.6



Enable the System

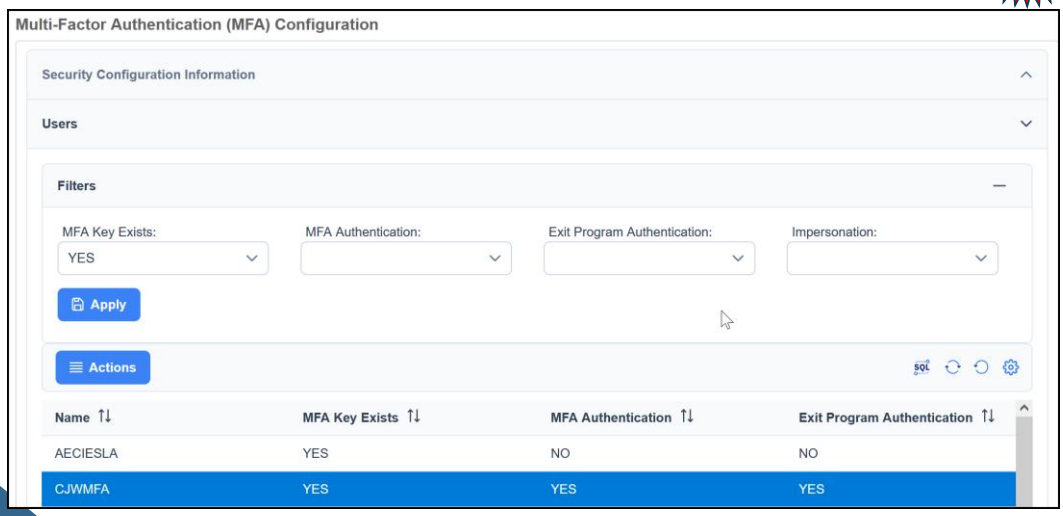
7.6



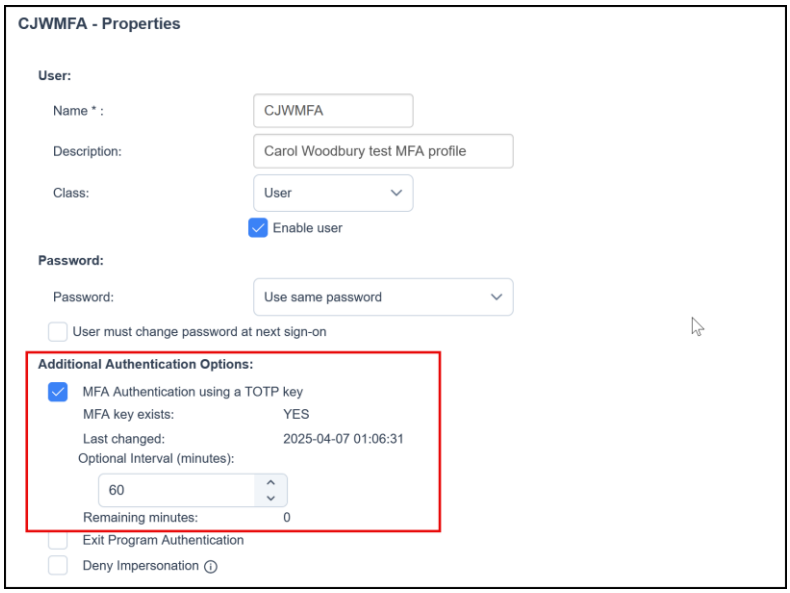
69

Configure / Manage Profiles

7.6



70



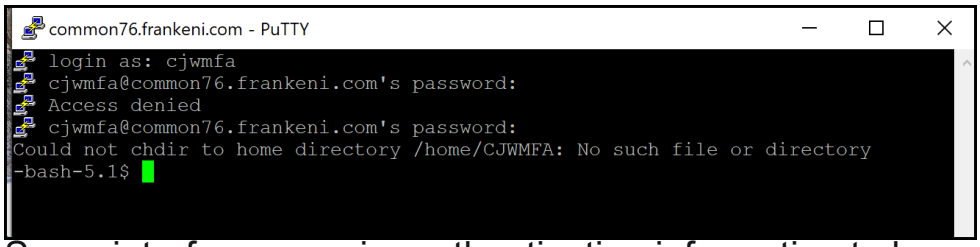
7.6

71

Why Use the Optional Interval?

7.6

- To avoid the awkwardness of some interfaces such as SSH:



- Some interfaces require authentication information to be entered as: password:additional_token

  St0ngPassw#rd:559012

72

IBM i MFA Considerations

7.6

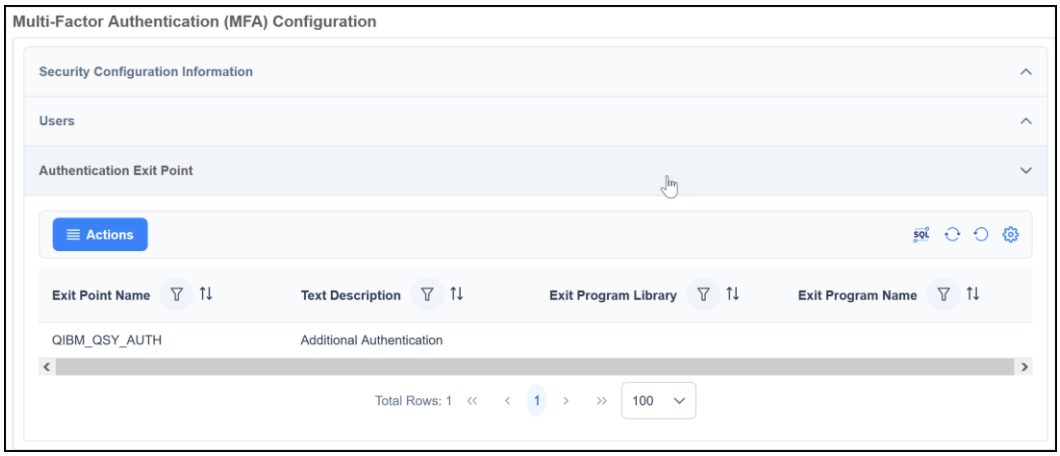
- Check compliance requirements prior to implementing Optional Interval
- MFA system enablement is a Security Attribute – NOT a system value
  - Value is NOT saved / restored!

kisco

73

Add the Program to the Exit Point

7.6



kisco

74

Using a Vendor's MFA Solution

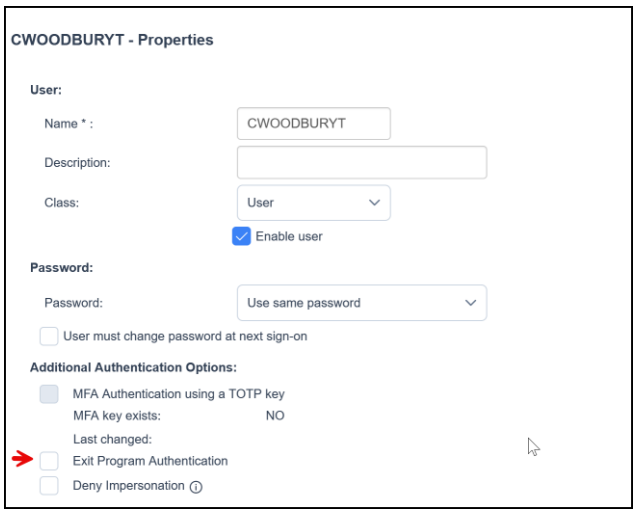
7.6

- Add the program to the QIBM_QSY_AUTH exit point
  - Exit point can use the additional factor from IBM i MFA or not
  - If not, the vendor solution can send a push notification for the additional factor
- Configure the users to use the exit point for MFA
- TOTP optional parm DOES NOT APPLY when only using exit point MFA.

75

Configure Profile to Use Exit Point Authentication

7.6



76

Finding Profiles with (or without) MFA Required

7.6

```
 4
 5 SELECT authorization_name,
 6        use_totp_authentication,
 7        totp_key_last_changed,
 8        totp_key_exists,
 9        totp_interval,
10        use_exit_program_authentication
11     FROM qsys2.user_info
12     WHERE use_totp_authentication = 'YES'
13           OR use_exit_program_authentication = 'YES';
```

Authorization Name	Use TOTP Authentication	TOTP Key Last Changed	TOTP Key Exists	TOTP Interval	Use Exit Program Authentication
AUTHORIZATION_NAME	USE_TOTP_AUTHENTICATION	TOTP_KEY_LAST_CHANGED	TOTP_KEY_EXISTS	TOTP_INTERVAL	USE_EXIT_PROGRAM_AUTHEI
CJWMFA	YES	2025-04-07 01:06:31	YES	0	YES

kisco

77

Redbook - Refresh

2014

Coming Soon!

“Modernizing IBM i Applications”

2026

78

kisco

78

For More Information

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

Memo to Users – 7.5 and 7.6

IBM i 7.6 Redbook - https://www.redbooks.ibm.com/redpieces/pdfs/sg248588.pdf

IBM i MFA - PDF

IBM i Security Reference – PDF

IBM i Security Administration and Compliance, 3nd edition, by Carol Woodbury, 2020
available from Amazon or MCPress Bookstore

Mastering IBM i Security – A Step by Step Approach by Carol Woodbury, 2022
available from Amazon or MCPress Bookstore

Whitepaper: Securing IBM i: A Dual Responsibility

Articles by Carol Woodbury on mcpressonline.com

Kisco U – free articles and tutorials, for example …
https://www.kisco.com/u/content/subscribe-to-ibm-notifications-for-ibm-i.html

79

kisco

79

System Service Tools (SST)

kisco

80

Locking Security-related Attributes

7.5

- Sign on to SST, choose option 7 = Work with system security

```
                    Work with System Security
                                                          System:   DXREX75
Type choices, press Enter.

  Allow system value security changes . . . . .  1  0=No, 1=Yes
  Allow new digital certificates  . . . . . .  1  0=No, 1=Yes
  Allow a service tools user ID with a
   default and expired password to change
   its own password . . . . . .  0  0=No, 1=Yes
  Allow add and remove of password exit programs 1  0=No, 1=Yes
```


Lock System Values

- Use SST (System Service Tools) or DST (Dedicated System Tools) to lock system values. The following system values can be locked:

QALWJOBITP	QAUTORMT	QLMTDEVSSN	QPWDLMTREP	QRETSVRSEC
QALWOBJRST	QAUTOVRT	QLMTSECOFR	QPWDLVL	QRMTSIGN
QALWUSRDMN	QCRTAUT	QMAXSGNACN	QPWDMAXLEN	QRMTSRVATR
QAUDCTL	QCRTOBJAUD	QMAXSIGN	QPWDMINLEN	QSCANFS
QAUDENDACN	QDEVRCYACN	QPWDCHGBLK	QPWDPOSDIF	QSCANFSCTL
QAUDFRCLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QSECURITY
QAUDLVL	QDSCJOBITV	QPWDEXPWRN	QPWDRQDDIF	QSHRMEMCTL
QAUDLVL2	QFRCCVNRST	QPWDLMTAJC	QPWDRULES	QUSEADPAUT
QAUTOCFG	QINACTMSGQ	QPWDLMTCHR	QPWDVLDPGM	QVFYOBJRST

- Note: Locking system values is “all-or-nothing”. You can’t lock some and leave others unlocked.

SST Commands Enhanced

7.5

```
CMDSST                    System Service Tools Commands

Select one of the following:

  Commands
     1. Change SST Security Attributes                          CHGSSTSECA
     2. Change Service Tools User ID                            CHGSSTUSR
     3. Create Service Tools User ID                            CRTSSTUSR
     4. Delete Service Tools User ID                            DLTSSTUSR
     5. Disp
     6. Disp
     7. Star
```

```
                Change SST Security Attributes (CHGSSTSECA)

Type choices, press Enter.

Requesting SST user ID . . . . .  _________   Character value
Requesting SST user ID pwd . . .
Service tools password level . .  2_____      Number, *SAME, 2, 3
Maximum sign-on attempts . . . .  3_____      2-15, *SAME
Password expiration interval . .  180___      1-366, *SAME, *NOMAX
Duplicate password control . . .  18____      1-32, *SAME, *NONE
Allow security sysval changes  .  *YES__      *SAME, *YES, *NO
Allow add of digital certs . . .  *YES__      *SAME, *YES, *NO
Allow SST password change  . . .  *NO___      *SAME, *YES, *NO
Add and remove pwd exit pgms . .  *YES__      *SAME, *YES, *NO
```

GO CMDSST

83

SST Users Removed

7.5

```
                        Display Service Tools User IDs
                                                              System:   DXREX74
Type options, press Enter.
  5=Display

Opt  DST/SST ID  Status      Linked      Description
     CAROL       *DISABLED               CAROL WOODBURY
_    LDB         *ENABLED                Larry "DrFranken" Bolhuis
_    QSECOFR     *ENABLED    QSECOFR     QSECOFR
_    QSRV        *DISABLED               QSRV
_    11111111    *ENABLED                11111111
_    22222222    *DISABLED               22222222
```

- 11111111 and 22222222 Service Tool IDs removed
- *BASIC and *FULL options removed when creating a service tool id

Check to See if Password Meets Rules

7.5

- QSYS2.CHECK_PASSWORD
- QSYCHKPR

- Checks password *prior* to changing to determine if it meets password rules.

85

Features: Validation Lists

86

Validation Lists

- Allows for secure storage of user and authentication information without creating an IBM i user profile
- APIs are available to check or retrieve authentication information

- “Internet users” – web application users
- Useful for storing passwords used for connections
- Other application users

87

Validation List SQL Interfaces

IBM i 7.5 TR5
IBM i 7.4 TR11

- SQL helper functions added:
  - SYSTOOLS.Add_Validation_List_Entry
  - SYSTOOLS.Change_Validation_List_Entry
  - SYSTOOLS.Delete_Validation_List_Entry

88