

What's New in IBM i Security

Carol Woodbury CISSP, CRISC



IBM i Security SME and Senior Advisor, Kisco Systems

carol@kisco.com



© Kisco Systems LLC, All Rights Reserved.

1

IBM's Commitment to 'Secure by Design'

[Home](#) / [Trust](#) / IBM Security and Privacy by Design

IBM Security and Privacy by Design

Discover how IBM designs security and privacy into the core of its products

[Read IBM security principles](#) →

<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>

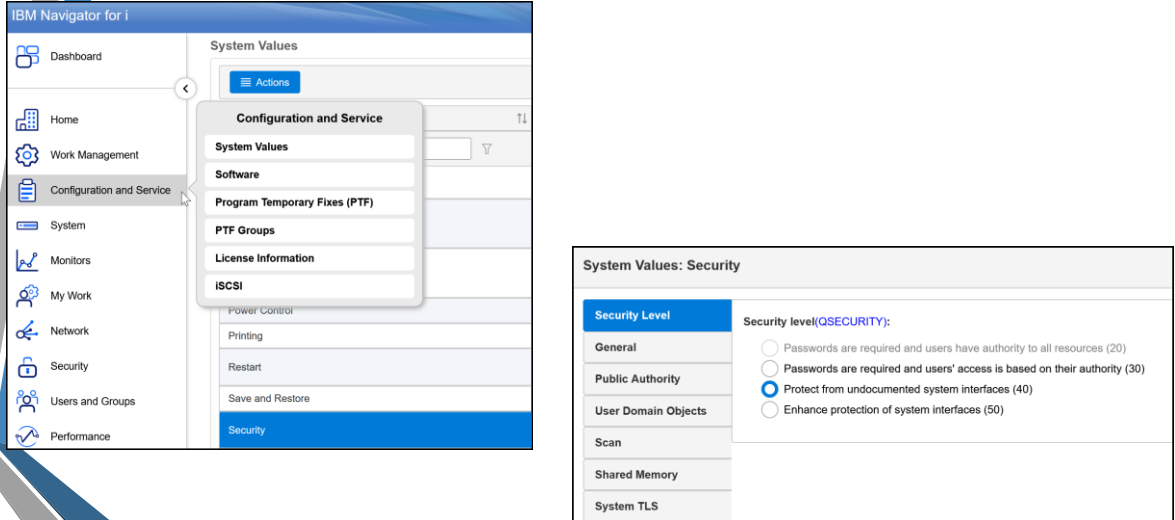
Whitepaper: [Securing IBM i: A Dual Responsibility](#)



Security Level and Auditing



QSECURITY – Security Level



The image shows the IBM Navigator for i interface. On the left is a navigation menu with options like Dashboard, Home, Work Management, Configuration and Service, System, Monitors, My Work, Network, Security, Users and Groups, and Performance. The 'Configuration and Service' menu is expanded, showing options like System Values, Software, Program Temporary Fixes (PTF), PTF Groups, License Information, ICSI, Power Control, Printing, Restart, Save and Restore, and Security. To the right, a 'System Values: Security' window is open, showing the 'Security level(QSECURITY):' setting. The current value is 40, indicated by a blue radio button. Other options include 20, 30, and 50, each with a radio button. The 'General' section is expanded, showing the following options:

Security Level	Security level(QSECURITY):
General	<input type="radio"/> Passwords are required and users have authority to all resources (20)
Public Authority	<input type="radio"/> Passwords are required and users' access is based on their authority (30)
User Domain Objects	<input checked="" type="radio"/> Protect from undocumented system interfaces (40)
Scan	<input type="radio"/> Enhance protection of system interfaces (50)
Shared Memory	
System TLS	

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

Authority Failure (AF) Detail View

Daily Summary View

Using Live Data Filters

Actions

Qualified Job Name ↑↓	Program Library ↑↓	Program Name ↓↑	Violation Type ↑↓	Violation Type Detail ↑↓	Object Lib
Filter	Filter	Filter	6 items selected	Filter	Filter
051096/CWOODBURY/QPADEV0005	QSYS	QCMD			

Selected Rows: 1 | Total Rows: 6

- Not Authorized to Object (A)
- Restricted Instruction (B)
- Validation Failure. See VALIDATION_ERROR_ACTION (C)
- Use of Unsupported Interface, Object Domain Failure (D)



7

Using AF Audit Helper Function to Move to Level 40

Run SQL Scripts - common76.franken1.com(Common76)

File Edit Search View Connection Run Explain Monitor Editor Tools Help

*Untitled 1

```

1 SELECT entry_timestamp,
2       user_name,
3       qualified_job_name,
4       program_library,
5       program_name,
6       violation_type,
7       violation_type_detail,
8       object_library,
9       object_name,
10      object_type,
11      program_instruction
12 FROM TABLE (
13   systools.audit_journal_af(starting_timestamp => CURRENT_TIMESTAMP - 7 DAYS)
14 )
15 WHERE violation_type IN ('B', 'C', 'D', 'U', 'R', 'S');
```

ENTRY_TIMESTAMP	USER_NAME	QUALIFIED_JOB_NAME	PROGRAM_LIBRARY	PROGRAM_NAME	VIOLATION_TYPE	VIOLATION_TYPE_DETAIL
2026-05-08 09:35:15.023808	CWOODBURY	051096/CWOODBURY/QPADEV0005	QSYS	QCMD	D	Use of unsupported interface, object domain failure

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



8

Audit Journal Entry SQL Table Functions

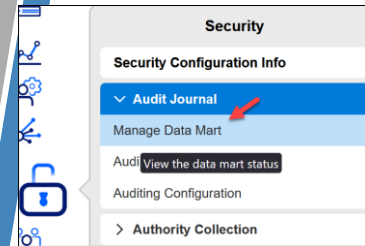
- Original helper functions included:
 - AF – Authority Failure (SYSTOOLS.AUDIT_JOURNAL_AF)
 - CA – Changes to Authority (SYSTOOLS.AUDIT_JOURNAL_CA)
 - OW – Ownership Changes (SYSTOOLS.AUDIT_JOURNAL_OW)
 - PW – Password (SYSTOOLS.AUDIT_JOURNAL_PW)
- Available beginning in V7R3 TR10 and V7R4 TR4
- Now, 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



IBM Navigator for i

Manage Audit Journal Data Mart

Data Mart Library	Journal Entry Type	Status	Audit Journal Starting Timestamp	Audit Journal Ending Timestamp
cwoodbury	Filter	Filter	Filter	Filter
CWOODBURY	Password (PW)	COMPLETED	2023-10-20 02:59:20.000000	2024-05-27 17:53:00.000000
CWOODBURY	User Profile Changes (CP)	COMPLETED	2024-05-20 00:00:00.000000	2024-05-27 21:26:48.359441
CWOODBURY	Action to System Value (SV)	COMPLETED	2024-05-24 15:22:32.000000	2024-05-27 15:22:32.000000



10

Create a New Audit Journal Data Mart

Create New Data Mart [X]

Data Mart Library:

Journal Entry Type: Authority Failure (AF) [v]

Action: Create a new data mart [v]

Audit Journal Starting Timestamp: Use the attach time for the oldest, attached journal receiver [v]

Audit Journal Ending Timestamp: 10/07/2024 12:03 AM [📅]

Data Mart Filter:

[OK] [Cancel]

11

Data Mart Options

Manage Audit Journal Data Mart

Actions [☰]

Data Mart	Data Mart Library
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>
AUDIT_JOURNAL_CP	CWOODBURY
AUDIT_JOURNAL_PW	CWOODBURY
AUDIT_JOURNAL_SV	

- Manage
- Delete
- Detail View
- Daily View
- Weekly View
- Schedule

Schedule [X]

Data Mart Library: CWOODBURY

Journal Entry Type: User Profile Changes (CP) [v]

Action: Append new data to the existing data mart [v]

Append new data to the existing data mart

Delete the existing data mart and create a new one

Delete entries from the data mart table

03/06/2025 08:31 AM [📅]

Data Mart Filter:

[OK] [Cancel]

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'
);
```



13

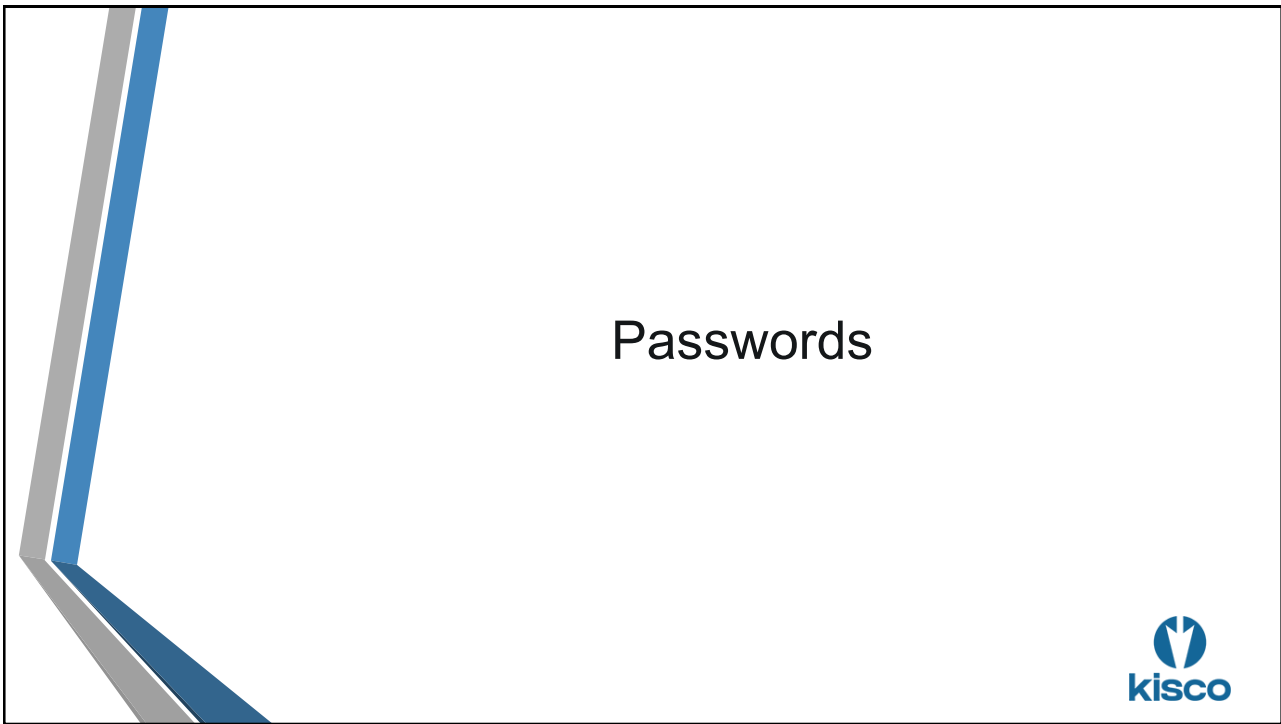
Data_Mart_Filter parm

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"');
```



14



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 <div style="text-align: center; margin-top: 5px;"> ➔ Default for new installs as of IBM i 7.6 </div>
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



Display System Value

System value : QPWDLVL
 Description : Password level

Password level : 3

Display System Value

System value : QPWDRULES
 Description : Password rules

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

NEW INSTALLS ONLY !!!



New Defaults in IBM i 7.6



System Values: Password

- General**
- Composition Rules
- Basic Composition Rules
- Expiration

Password level (current):
 Long passwords using an unlimited character set (4)

- Password level (at next restart)(QPWDLVL):
- Short passwords using a limited character set (0)
 - "Short passwords using a limited character set (1) *"
 - Long passwords using an unlimited character set (2)
 - "Long passwords using an unlimited character set (3)
 - Long passwords using an unlimited character set (4)

← New default in IBM i 7.6

System Values: Password

- General
- Composition Rules**

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.

- Restrict user profile in password
- Require a minimum number of lowercase and uppercase letters (0-9):
 -
- Require characters from at least 3 of the following types of characters (upper, lower, digit, special)
- Enforce all password validation options when creating or changing a password with CRTUSRPRF or CHGUSRPRF.



Password Hashes Stored at Each Level

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

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



Same Message Issued for Incorrect User or Password



```

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



Press F9 to View the Rules!



```

Change Password
User profile . . . . . : CWOODBURY
Password last changed . . . . . :
Type choices, press Enter.
Current password . . . . .
New password . . . . .
New password (to verify) . . . . .

F3=Exit          F9=Display password rules  F12=Cancel
  
```



User Profiles



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



```

Create User Profile (CRTUSRPRF)
Type choices, press Enter.
User profile . . . . . newprofile      Name
User password . . . . . *NONE
Set password to expired . . . . . *yes
Status . . . . . *ENABLED           *NO, *YES
User class . . . . . *USER           *ENABLED, *DISABLED
Assistance level . . . . . *SYSVAL   *USER, *SYSOPR, *PGMR...
Current library . . . . . *CRTDFT    *SYSVAL, *BASIC, *INTERMED...
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!!!
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



Create User Profile – 2 (new Parm)



```

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, *TYPEHEAD...
Maximum allowed storage large . . *NOMAX
Maximum allowed storage . . . . *NOMAX Kilobytes, *NOMAX
Highest schedule priority . . . . 3      0-9
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
  
```



Create and Manage Profiles in Navigator for i

The screenshot shows the IBM Navigator for i interface. The main window displays a table of users with columns for Name, Status, Special Authorities, Description, Group, and Supplemental Groups. A search filter 'cwood' is applied to the Name column. The Actions menu is expanded, showing options like 'New User (based on)', 'Delete', 'Copy to System', 'Send Message', 'User Objects', 'Authority Collection', 'Properties', 'New User', 'Export Selected', 'Export All', 'Select All', and 'Deselect All'.

Name	Status	Special Authorities	Description	Group	Supplemental Groups
CWOODBURYC	*ENABLED	*JOBCTL	Carol test profile	QPGMR	
CWOODBURYT	*ENABLED	*JOBCTL		QPGMR	
CWOODBURYZ	*ENABLED	*ALLOBJ *SECADM *JOBCTL *SPLCTL *SAVSYS *SERVICE *AUDIT *IOSYSCFG	Carol Woodbury test profile	*NONE	

26

Find Profiles with *IOSYSCFG using qsys2.user_info

The screenshot shows a SQL query editor with the following query:

```

20 -- category: IBM / Services
21 -- description: Modified from ACS - Insert from Examples: Security - Review *ALLOBJ users |
22 --
23 -- Which users have *IOSYSCFG authority either directly
24 -- or via a Group or Supplemental profile?
25 --
26 SELECT AUTHORIZATION_NAME,
27        STATUS,
28        NO_PASSWORD_INDICATOR,
29        LAST_USED_TIMESTAMP,
30        PREVIOUS_SIGNON,
31        TEXT_DESCRIPTION
32 FROM QSYS2.USER_INFO
33 WHERE SPECIAL_AUTHORITIES LIKE '%*IOSYSCFG%'
34    OR AUTHORIZATION_NAME IN (SELECT USER_PROFILE_NAME
35                             FROM QSYS2.GROUP_PROFILE_ENTRIES
36                             WHERE GROUP_PROFILE_NAME IN (SELECT AUTHORIZATION_NAME
37                                                           FROM QSYS2.USER_INFO
38                                                           WHERE SPECIAL_AUTHORITIES LIKE '%*IOSYSCFG%'))
39 ORDER BY AUTHORIZATION_NAME;

```

The results table is as follows:

Authorization Name	Status	No Password Indicator	Last Used Timestamp	Previous Signon	Text Description
AUTHORIZATION_NAME	STATUS	NO_PASSWORD_INDICATOR	LAST_USED_TIMESTAMP	PREVIOUS_SIGNON	TEXT_DESCRIPTION
APILABMAIN	*ENABLED	NO	2025-09-17 00:00:00.000000	2025-09-17 08:09:14.000000	CPDS API Lab
APILAB88	*ENABLED	NO	2025-08-29 00:00:00.000000	2025-08-29 09:34:34.000000	CPDS API Lab
ASHEDIVY	*ENABLED	NO	-	-	-
BRAD	*DISABLED	NO	2023-06-09 00:00:00.000000	2023-06-09 11:21:44.000000	Sir Steve of Bradshaw
BRIANJAS	*ENABLED	NO	2025-12-28 00:00:00.000000	2025-12-28 15:31:25.000000	AJS Test User cor Brian
CGUARINO	*ENABLED	NO	2026-04-08 00:00:00.000000	2026-04-08 17:10:04.000000	Charles Guarino of IBM Fame, Champion, Friend,
CJWPUBLIC	*DISABLED	YES	2025-08-25 00:00:00.000000	-	Powerful profile not *EXCLUDE

27

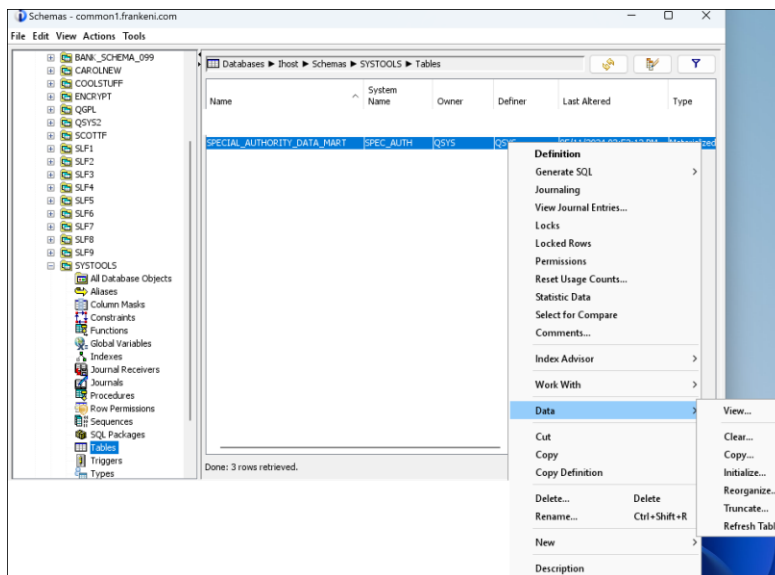
IBM i 7.6 Memo to Users (MTU) - *IOSYSCFG Expanded

- 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



28

SYSTOOLS.Special_Authority_Data_Mart



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 extraordinaire	2026-01-13
TIMMR	GROUP PROFILE	SUPERUSER	*ENABLED	Tim M Rowe - IBM Presentor extraordinaire	2026-01-13



Increased Use of Function Usage



Function Usage (previously Application Administration)

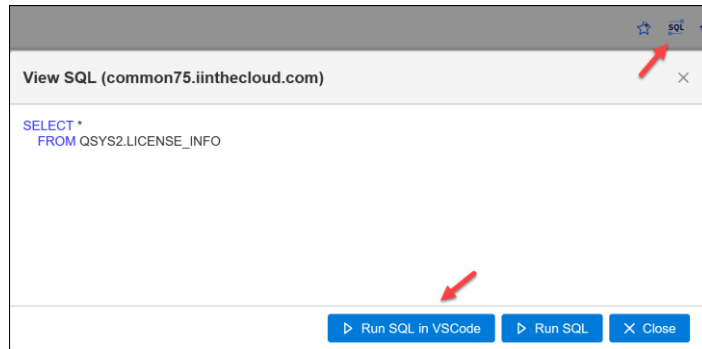
The screenshot shows a web interface titled 'Function Usage'. It features a table with columns: Function ID, Function Name, Group ID, Description, Default Usage, All Object Indicator, and Profiles A Denied. A 'Security' dropdown menu is open, listing options like 'Security Configuration Info', 'Authorization Lists', 'Function Usage', 'Network Authentication Service', 'Enterprise Identity Mapping (EIM)', and 'IBM Digital Certificate Manager for i'. A tooltip points to the 'Function Usage' option, stating: 'Work with function usage, also known as the Application Administration support in the past'.

Function ID	Function Name	Group ID	Description	Default Usage	All Object Indicator	Profiles A Denied
QIBM_NAV_WRK_MGT	WORK MANAGEMENT	*NONE		ALLOWED	USED	NO
QIBM	CONFIGURATION AND	*NONE		ALLOWED	USED	NO
		*NONE		ALLOWED	USED	NO
		*NONE		ALLOWED	USED	NO
		*NONE		ALLOWED	USED	NO
		*NONE		ALLOWED	USED	NO

- 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



It's Not Just ACS Anymore!



Function Usage in Navigator for i

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

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

36

36

QIBM_IOSYSCFG_VIEW function



Function ID	Description	Default Usage	All Object Indicator
QIBM_IOSYSCFG_VIEW	Allows the ability to view Input/Output system configuration information.	DENIED	NOT USED

Total Rows: 1

Usage options for the selected function IDs

Default authority: Denied

*ALLOBJ special authority: Not used

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

Profile(s): [Browse Profiles](#)

Access Allowed: [Add](#) [Remove](#)

Access Denied: [Add](#) [Remove](#)

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

37

QIBM_RUN_UNDER_NO_AUTH



Function ID	Description	Default Usage	All Object Indicator
QIBM_RUN_UNDER_USER_NO_AUTH	Run under a user without verifying the authentication information for the user	ALLOWED	NOT USED

Total Rows: 1

Usage options for the selected function IDs

Default authority:

*ALLOBJ special authority:

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

Profile(s):

Access Allowed:

Access Denied:

Allows you to protect 'powerful' profiles from being exploited

40

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 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



44

New IBM-Supplied User Profiles



- 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!



45

Emphasis on Using Secure Ports



IBM i 7.5 TR5
IBM i 7.4 TR11

Not Secure 129.40.98.201:2002/Navigator/mainframe/dashboard-card

Warning: NAV_209003: Your connection to the ADMIN1 server is using an unsecured port. It is recommended that you turn on Transport Layer Security (TLS) for the ADMIN1 server. Go to [Network > Web Administration > Application Servers > ADMIN1 > Configure TLS](#) to configure TLS for the ADMIN1 server.

Admin1 - Configure TLS Wizard

Basic Configuration

TLS Port Number:

TLS Protocol:

Disable non-TLS port:

- 1 Select Certificate Store
- 2 Specify the Password for the Certificate Store
- 3 Select truststore
- 4 Enter truststore password
- 5 Add trusted CA certificates
- 6 Specify Digital Certificate for TLS
- 7 Specify Ciphers for TLS
- 8 Restart the server
- 9 Summary

46

Easy to Turn off Unsecure Ports!



TLS Configuration

Deactivate Unsecure Port

Select Servers

Restart Servers

Secure Connections

Select All

TCP/IP Servers

- DDM (446)
- Telnet (23)
- DRDA Server (447)
- LDAP - QUSRDIR (389)

Admin Servers

- ADMIN (HTTP) (2001)
- Admin2 (Tivoli GUI) (2004)
- Admin5 (Remote System Explorer APIs) (2011)
- Admin1 (Navigator for i) (2002)
- Admin3 (DCM & Db2 Mirror) (2006)

Host Servers

- Central (8470)
- Data Queue (8472)
- Net Print (8474)
- Sign On (8476)
- Database (8471)
- File (8473)
- Remote Command (8475)

Network->Servers->TLS Configuration

47

Emphasis on Using Encrypted (TLS) Sessions

Warning: NAV_201001: Connection is not secured with TLS. It is recommended that only secure connections be used when connecting to an IBM i. Go to [Serviceability > Connection Properties > TLS Connection](#) to secure all connections between the GUI and managed nodes.

IBM i 7.5 TR5
IBM i 7.4 TR11

Node	TLS Enablement	Use TLS For All Users
common1.iinthecloud.com	Off On	<input type="checkbox"/>
common75.iinthecloud.com	Off On	<input checked="" type="checkbox"/>
common75.frankeni.com	Off On	<input type="checkbox"/>
common76.frankeni.com	Off On	<input checked="" type="checkbox"/>

Dashboard view -> Serviceability -> Connection Properties

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

New Security-Focused Run SQL – Insert Examples

The screenshot shows a window titled "Examples" with a tab labeled "inject". On the left is a list of 39 security-related items, with "Security - Users with Limited Capabilities" selected. On the right, two SQL queries are displayed:

```
-- category: IBM i Services
-- description: Security - Commands that Limited Capabilities can use
-- Use Db2 for i to inject more Security into your IBM i
-- minvrm: v7r3m0

--
-- Which commands can be executed by users with "Limited Capabilities"?
SELECT *
FROM qsys2.command_info
WHERE allow_limited_user = 'YES';

-- category: IBM i Services
-- description: Security - Users with Limited Capabilities
-- Use Db2 for i to inject more Security into your IBM i
-- minvrm: v7r3m0

--
-- Which users are configured with "Limited Capabilities"?
SELECT *
FROM qsys2.user_info_basic
WHERE limit_capabilities = 'YES';
```

39 SQL statements available as of ACS 1.1.9.12!!!



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 *****



Protecting the System from Malware



52

File Shares !!!



IBM i



53

File Shares

Server Share Name	Path Name	Path Availability	Current Users	Permissions	Encryption Required	Authorization List
ASHARE2ROOT	/	Available	0	*RW	NO	
CAROLSHARE	/home/cjdemo	Available	0	*RW	NO	CAROLSHARE
CLAIMIMAGE	/claimimage	Available	0	*R	NO	
COMMON	/COMMON	Available	0	*R	NO	
HOMELDB	/home/ldb	Available	0	*R	NO	
IFSLAB06	/ifslab06	Available	0	*RW	NO	
IFSLAB08	/ifslab08/reflab	Available	0	*R	NO	
IFSLAB10	/ifslab10	Available	0	*RW	NO	
IFSLAB12	/ifslab12	Available	0	*RW	NO	
File System		Available	0	*RW	NO	
Integrated File System		Available	0	*RW	NO	
File Shares		Available	0	*R	NO	

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



54

Controlling Access to NetServer with an *AUTL



IBM i NetServer Properties

Security

Guest user ID:

Authentication method: Encrypted passwords:

Allow authentication with LAN Manager password hash:

Require clients to sign requests: Encrypted passwords:

Encrypt connections: Encrypted passwords:

Authorization List:

Buttons: Collapse Next Start, 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!

55

Secure Individual Shares with an *AUTL

7.5

Create IBM i NetServer File Share

General
IBM i Support for Windows Network Neighborhood

Share name:

Description:

Access: ▾

Encryption required: ▾

Authorization list:

Path name:

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?



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	-



58

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;

```



59



Multi-factor Authentication (MFA)



61

System Value Requirements for IBM i MFA



- System requirements:
 - QSECURITY 40 or 50
 - QPWDLVL 4 (!)



62

Step 1: Enable the System for IBM i MFA



```

Change Security Attributes (CHGSECA)

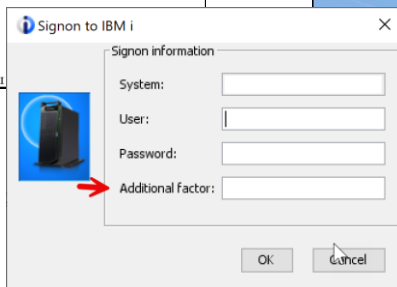
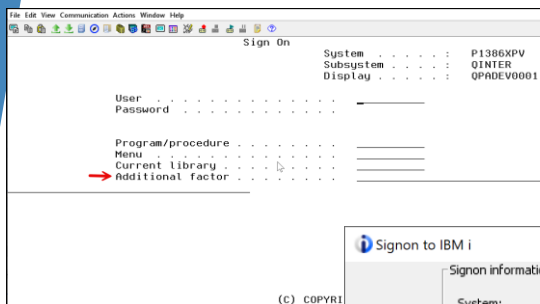
Type choices, press Enter.

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!



Signon Displays after IPL



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



Step 2: User Enrollment



Manage My MFA Key

Manage the Multi-factor Authentication (MFA) key for the user that is currently signed in to the GUI. The MFA key can only be generated, specified, removed, or validated by the signed-in user. This MFA key is a Time-Based One-Time Password (TOTP) key that is used with a client application to generate a MFA code. The MFA code is then paired with the User and Password when authenticating to a system that is leveraging MFA.

A MFA key does not exist for this user profile

- Generate and save a MFA key and recovery key for this user profile
- Enter a MFA key from your client generator application
- Remove the MFA key for this user profile
- Validate the MFA code and password work correctly for this user profile

[Next](#)

What users not authorized to Navigator for i will see

Warning: This profile has been restricted through function Usage ID QIBM_NAV_ALL_FUNCTION and has no further access to Navigator. Login with a user that has the required authority or contact your administrator for more access.



Scan the QR code and Verify




Validate MFA Key and Save Recovery Key

The new MFA key has been saved to your user profile. Validate that the MFA code allows this user profile to sign on, and then save the recovery key.

1. Saved MFA Key:
Using your client generator application, enter the MFA key below (without blanks) or scan the QR code

52ZSIAC32UZRUJ2Q2WP4LY43FPUKQ5GI

52ZS IAC3 2UZRU UB2Q 2WP4 LY43 FPUK Q5GI



2. Validate MFA Key:
Enter your user profile password and the MFA code from your client generator application to validate that your user profile can sign on with MFA

Password:

MFA Code:

[Validate](#)

3. Recovery Key:
Save the recovery key in a safe place, it can be used in place of the additional factor for recovery if the MFA key and code are not working

3150F99376CB6FAE449C49D8D0AB129A750F393E3B37757DD4D592D09F191319

[OK](#)

Use Okta, DUO, Microsoft Authenticator, etc



Step 3: Modify the User's Profile



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	*SAME, *NONE, *TOTP, *REGFAC
TOTP optional interval	60	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 ☺




Enable the System



Multi-Factor Authentication (MFA) Configuration

Security Configuration Information

Actions

Name	Current Value	Possible Values	Description
Additional Signon Factor	ENABLED	DISABLED, ENABLED	The current value of the additional sign-on factor security attribute. Can be changed using the Change Security Attributes (CHGSECA) command.
Allow Additional Signon Factor Change	YES	YES, NO	Whether the additional sign-on factor security attribute is allowed to be changed using the Change Security Attributes (CHGSECA) command. The Change Security Attributes (CHGSSTSECA) command can be used to change this attribute.
Allow Password Exit Program Add Remove	YES	YES, NO	Whether exit programs are allowed to be added to the QIBM_QSY_CHK_PASSRD, QIBM_QSY_VLD_PASSWRD, and QIBM_QSY_AUTH exit points with the Add Exit Program (ADDEXITPGM) command and the Add Exit Program (QUSDEP, QusAddExitProgram) API, and removed from the exit points with the Remove Exit Program (RMVEXITPGM) command and Remove Exit Program (QUS



69

Configure / Manage Profiles



Multi-Factor Authentication (MFA) Configuration

Security Configuration Information

Users

Filters

MFA Key Exists: YES
 MFA Authentication:
 Exit Program Authentication:
 Impersonation:

Apply

Actions

Name	MFA Key Exists	MFA Authentication	Exit Program Authentication
AECIESLA	YES	NO	NO
CJWMFA	YES	YES	YES



70

CJWMFA - Properties

User:

Name * : CJWMFA

Description: Carol Woodbury test MFA profile

Class: User

Enable user

Password:

Password: Use same password

User must change password at next sign-on

Additional Authentication Options:

MFA Authentication using a TOTP key

MFA key exists: YES

Last changed: 2025-04-07 01:06:31

Optional Interval (minutes): 60

Remaining minutes: 0

Exit Program Authentication

Deny Impersonation ⓘ



71

Why Use the Optional Interval?

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

```

common76.frankeni.com - PuTTY
login as: cjwmfa
cjwmfa@common76.frankeni.com's password:
Access denied
cjwmfa@common76.frankeni.com's password:
Could not chdir to home directory /home/CJWMFA: No such file or directory
-bash-5.1$ █
  
```

- Some interfaces require authentication information to be entered as:


```
password:additional_token
St0ngPassw#rd:559012
```



72

IBM i MFA Considerations



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



73

Add the Program to the Exit Point



Multi-Factor Authentication (MFA) Configuration

Security Configuration Information

Users

Authentication Exit Point

Actions

Exit Point Name	Text Description	Exit Program Library	Exit Program Name
QIBM_QSY_AUTH	Additional Authentication		

Total Rows: 1



74

Using a Vendor's MFA Solution

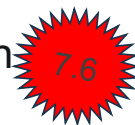


- Add the program to the QIBM_QSY_AUTH exit point
 - Exit point can use the additional factor from IBM i MFA or not
 - If not, the vendor solution can send a push notification for the additional factor
- Configure the users to use the exit point for MFA
- TOTP optional parm DOES NOT APPLY when only using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



75

Configure Profile to Use Exit Point Authentication



CWOODBURYT - Properties

User:

Name * : CWOODBURYT

Description:

Class: User

Enable user

Password:

Password: Use same password

User must change password at next sign-on

Additional Authentication Options:

MFA Authentication using a TOTP key
MFA key exists: NO

Last changed:

Exit Program Authentication

Deny Impersonation



76

Finding Profiles with (or without) MFA Required



```

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_AUTHEN
CJWMFA	YES	2025-04-07 01:06:31	YES		0 YES



Redbook - Refresh



2014



2026



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](#), 3rd 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 mcpresonline.com

[Kisco U](#) – free articles and tutorials, for example ...
<https://www.kisco.com/u/content/subscribe-to-ibm-notifications-for-ibm-i.html#g>



System Service Tools (SST)





Locking Security-related Attributes

- 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:

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

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



SST Commands Enhanced



```

CMSDST                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

```

```

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 CMSDST



SST Users Removed



```

Display Service Tools User IDs                System:  DXREX74

Type options, press Enter.
5=Display

Opt DST/SST ID  Status   Linked   Description
-  CAROL        *DISABLED
-  LDB          *ENABLED
-  QSECOFR      *ENABLED  QSECOFR  QSECOFR
-  QSRV         *DISABLED  QSRV     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



- 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



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



88