Achieving compliance with the latest IBM i security features

Thomas Barlen
Senior Managing Consultant
barlen@de.ibm.com
IBM Systems Lab Services & Training

IBM Systems Lab Services

COMMON, Luxemburg
23. May 2019

Agenda

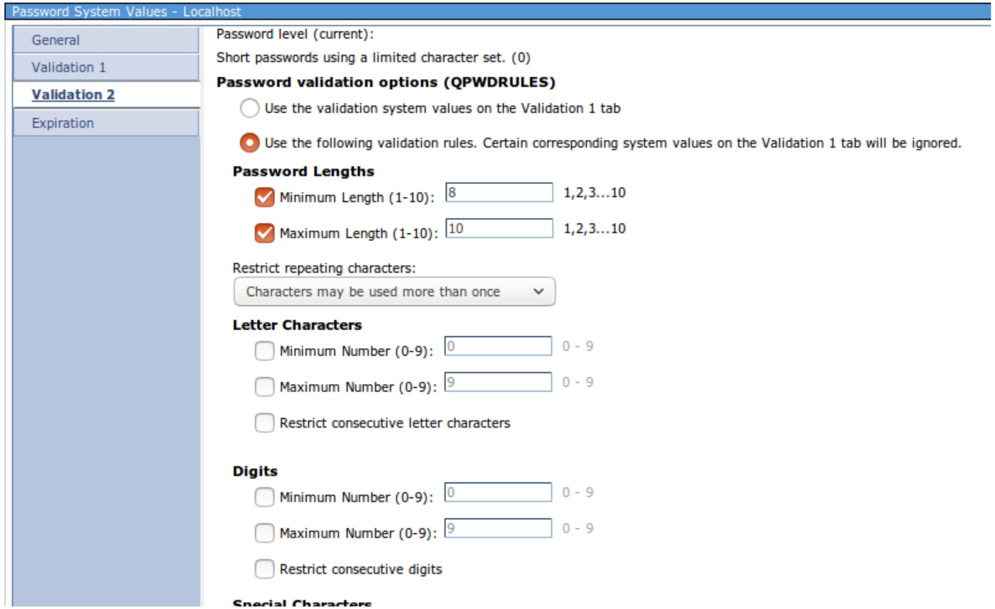
- Base IBM i security enhancements
- Access Control security enhancements
- Database security enhancements
- Network security enhancements

Agenda

- Base IBM i security enhancements
- Access Control security enhancements
- Database security enhancements
- Network security enhancements

QPWDRULES Password rules

NOTE: Validation tab 2
are the combined password rules
when using the QPWDRULES system
value



Password System Values - Localhost

Password level (current):
Short passwords using a limited character set. (0)

Password validation options (QPWDRULES)

○ Use the validation system values on the Validation 1 tab

● Use the following validation rules. Certain corresponding system values on the Validation 1 tab will be ignored.

Password Lengths

☑ Minimum Length (1-10): 8 1,2,3...10

☑ Maximum Length (1-10): 10 1,2,3...10

Restrict repeating characters:
Characters may be used more than once

Letter Characters

☐ Minimum Number (0-9): 0 0 - 9

☐ Maximum Number (0-9): 9 0 - 9

☐ Restrict consecutive letter characters

Digits

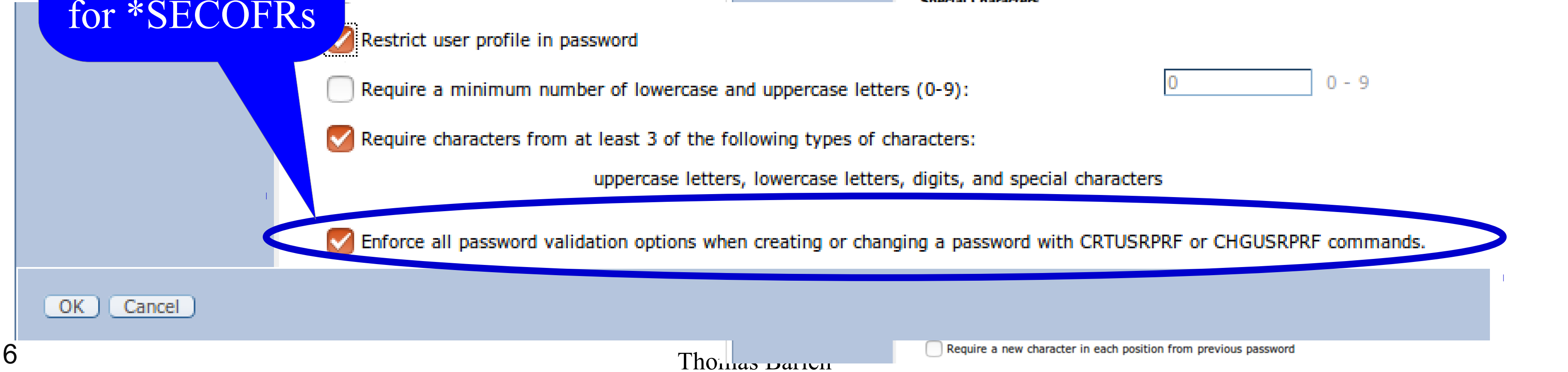
☐ Minimum Number (0-9): 0 0 - 9

☐ Maximum Number (0-9): 9 0 - 9

☐ Restrict consecutive digits

Special Characters

Enforces password policies also for *SECOFRs



☑ Restrict user profile in password

☐ Require a minimum number of lowercase and uppercase letters (0-9): 0 0 - 9

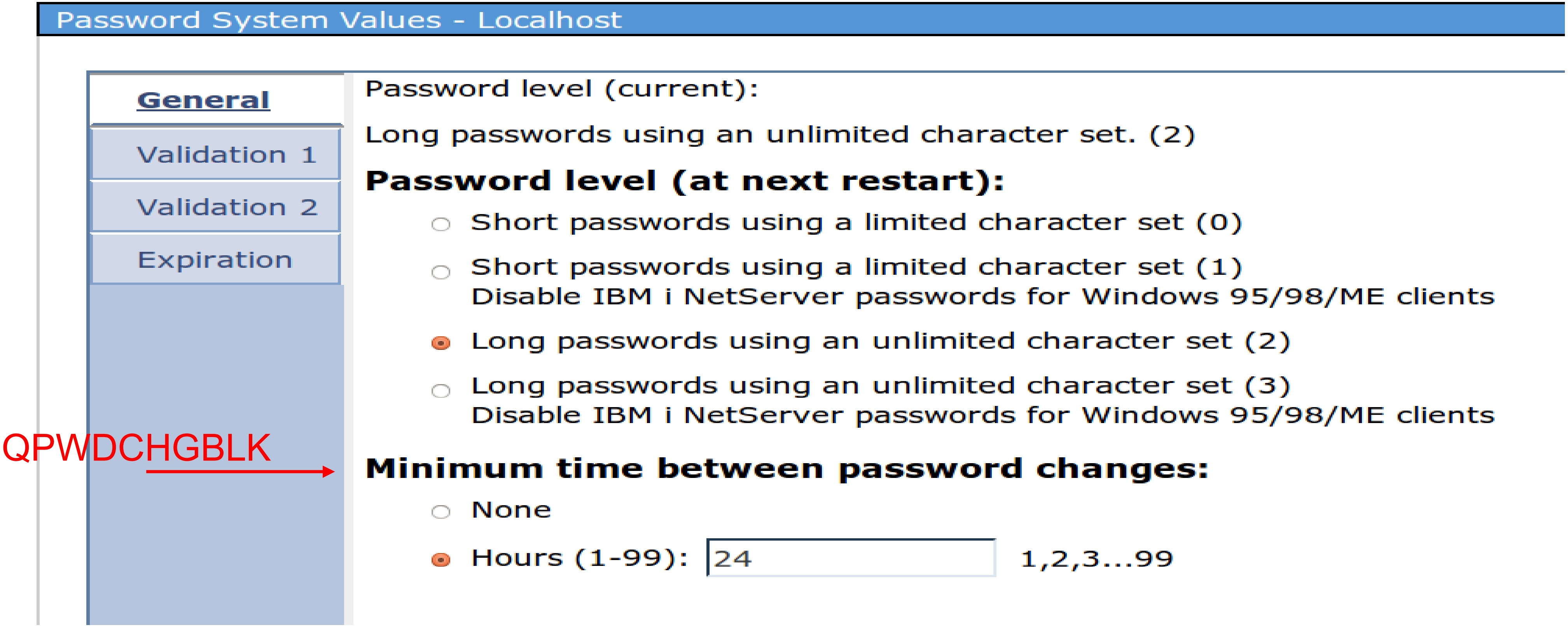
☑ Require characters from at least 3 of the following types of characters:

uppercase letters, lowercase letters, digits, and special characters

☑ Enforce all password validation options when creating or changing a password with CRTUSRPRF or CHGUSRPRF commands.

☐ Require a new character in each position from previous password

QPWDCHGBLK – Password Change Block



Password System Values - Localhost

Password level (current):

Long passwords using an unlimited character set. (2)

Password level (at next restart):

○ Short passwords using a limited character set (0)

○ Short passwords using a limited character set (1)
Disable IBM i NetServer passwords for Windows 95/98/ME clients

● Long passwords using an unlimited character set (2)

○ Long passwords using an unlimited character set (3)
Disable IBM i NetServer passwords for Windows 95/98/ME clients

Minimum time between password changes:

○ None

● Hours (1-99): 24 1,2,3...99

QPWDCHGBLK

Password validation exit program

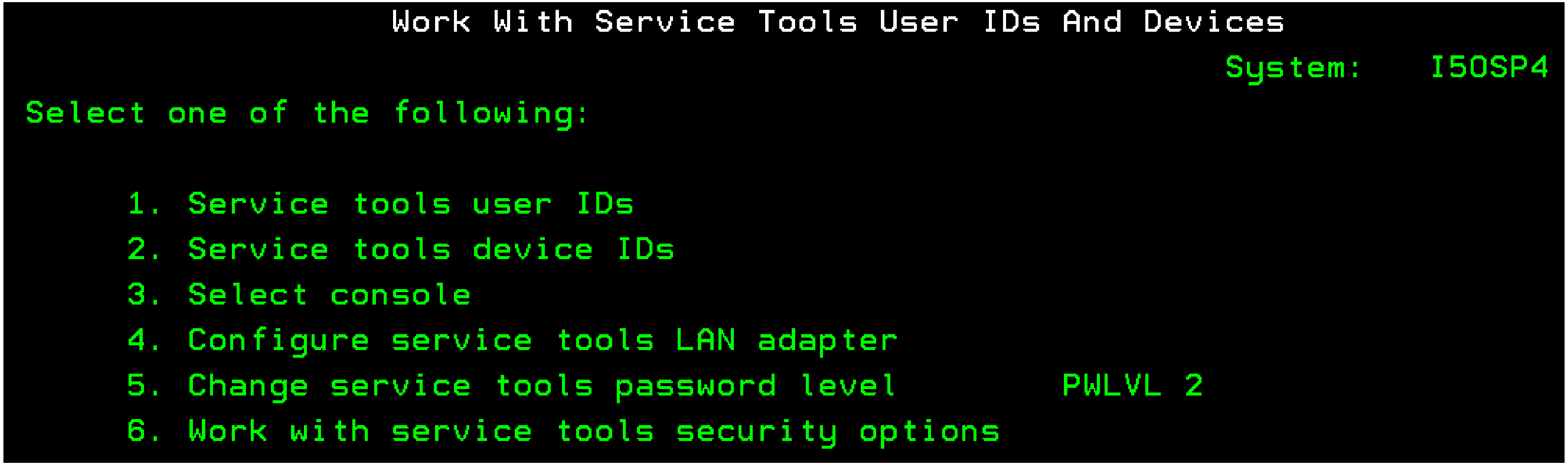
7.4

- Exit point and QPWDVLDPGM system value behavior changes
  - When running in a system job, subsystem job or the SCPF job, exit programs will not be called for the program specified for the QPWDVLDPGM system value or for exit points:
    - QIBM_QSY_VLD_PASSWRD
    - QIBM_QSY_CHK_PASSWRD
    - QIBM_QSY_RST_PROFILE
    - QIBM_QSY_CHG_PROFILE
    - QIBM_QSY_DLT_PROFILE
    - QIBM_QSY_CRT_PROFILE

Service tools enhancements

7.4

- Additional password rules have been introduced for the DST / SST environment
  - The new rules are based on the password rules (QPWDRULES) system value
  - Rules are only enabled when the service tools password level is 2

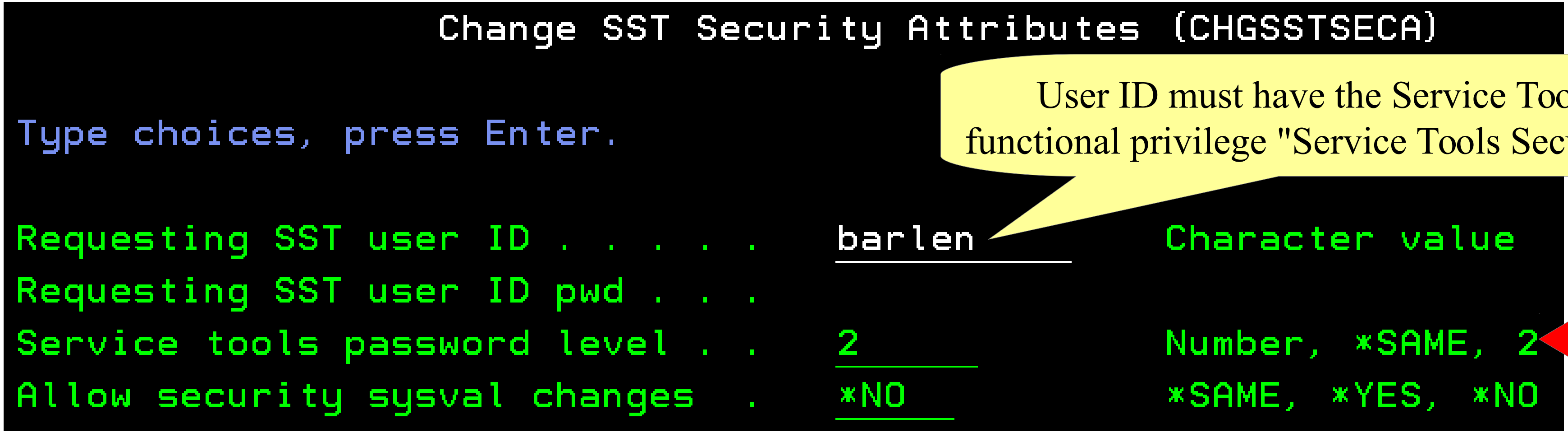


```
                  Work With Service Tools User IDs And Devices
                                                       System:   I50SP4
Select one of the following:

     1. Service tools user IDs
     2. Service tools device IDs
     3. Select console
     4. Configure service tools LAN adapter
     5. Change service tools password level       PWLVL 2
     6. Work with service tools security options
```

Service tools enhancements (cont'd)

7.4

- SST / DST password level and rules can also be changed via new CL command
  - Change SST Security Attributes (CHGSSTSECA)



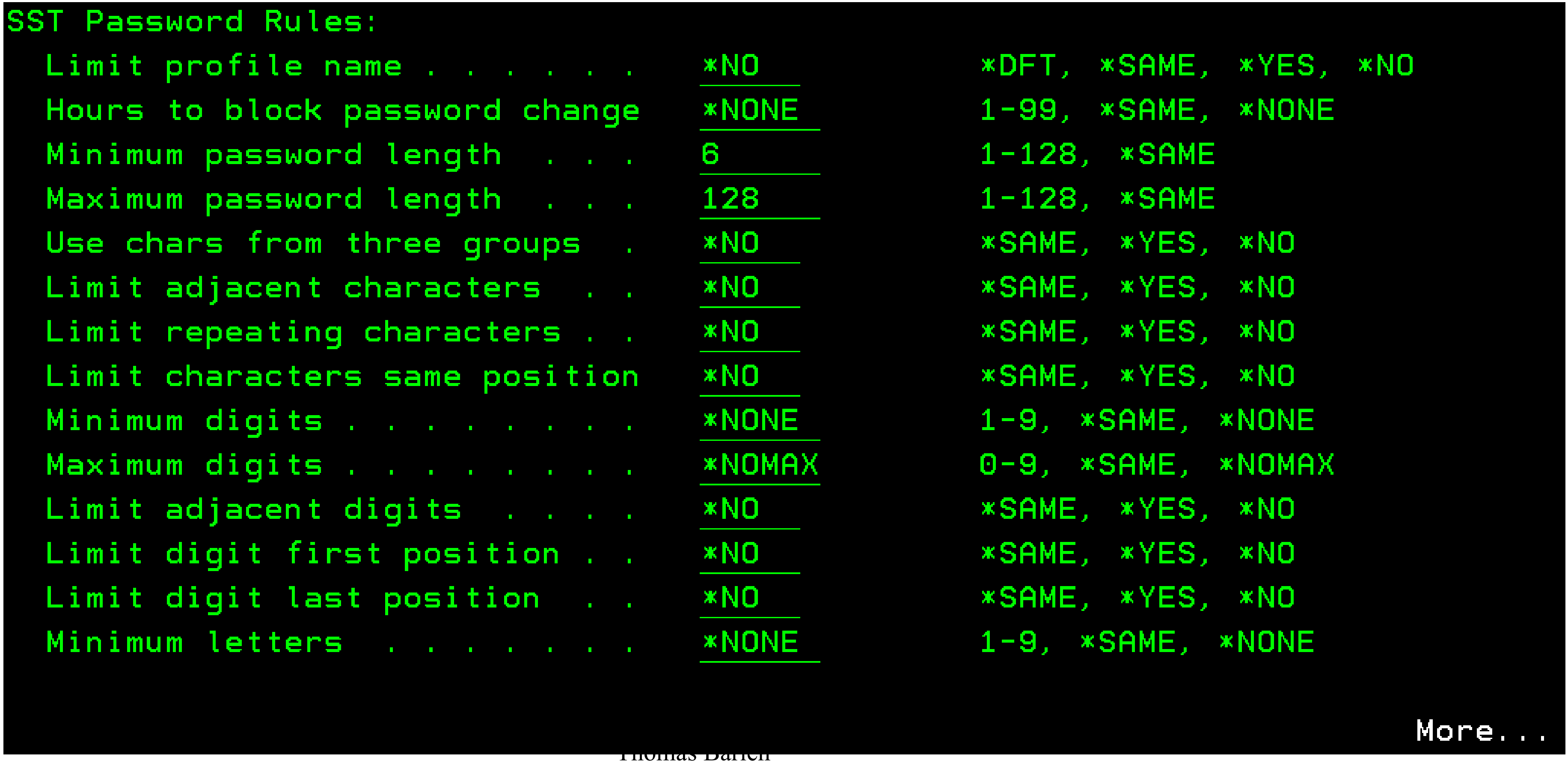
```
                    Change SST Security Attributes (CHGSSTSECA)

Type choices, press Enter.

Requesting SST user ID . . . . .   barlen          Character value
Requesting SST user ID pwd . . .
Service tools password level . .   2               Number, *SAME, 2
Allow security sysval changes  .   *NO             *SAME, *YES, *NO
```

User ID must have the Service Tool user functional privilege "Service Tools Security".

Service tools enhancements (cont'd)

7.4

- Change SST Security Attributes (CHGSSTSECA)

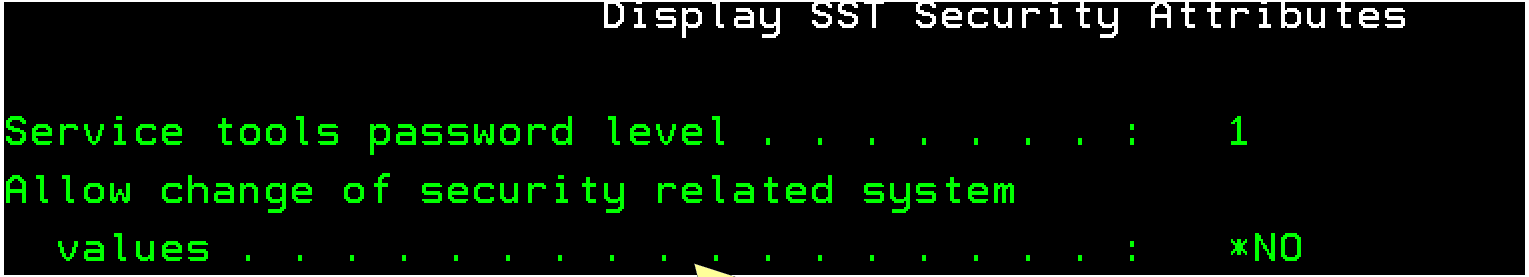


```
SST Password Rules:
  Limit profile name . . . . . . .   *NO             *DFT, *SAME, *YES, *NO
  Hours to block password change     *NONE           1-99, *SAME, *NONE
  Minimum password length  . . .     6               1-128, *SAME
  Maximum password length  . . .     128             1-128, *SAME
  Use chars from three groups  .     *NO             *SAME, *YES, *NO
  Limit adjacent characters  . .     *NO             *SAME, *YES, *NO
  Limit repeating characters . .     *NO             *SAME, *YES, *NO
  Limit characters same position     *NO             *SAME, *YES, *NO
  Minimum digits . . . . . . . .     *NONE           1-9, *SAME, *NONE
  Maximum digits . . . . . . . .     *NOMAX          0-9, *SAME, *NOMAX
  Limit adjacent digits  . . . .     *NO             *SAME, *YES, *NO
  Limit digit first position . .     *NO             *SAME, *YES, *NO
  Limit digit last position  . .     *NO             *SAME, *YES, *NO
  Minimum letters  . . . . . . .     *NONE           1-9, *SAME, *NONE


                                                                  More...
```

Service tools enhancements (cont’d)

7.4

- More new SST / DST related commands
  - Display SST Security Attrs (DSPSSTSECA)



```
                    Display SST Security Attributes

Service tools password level . . . . . . . . :   1
Allow change of security related system
  values . . . . . . . . . . . . . . . . . . :   *NO
```

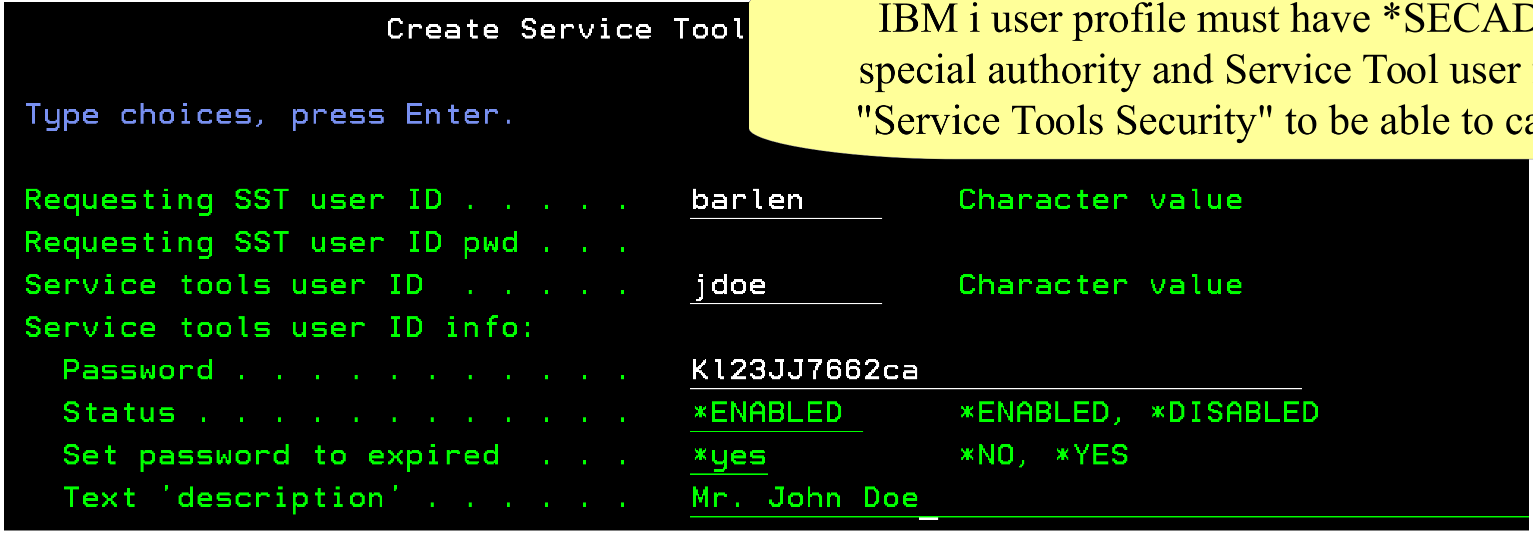
IBM i user profile must have *SECADM or *AUDIT special authority to be able to call this CL command

Service tools enhancements (cont'd)

7.4

- More new SST / DST related commands to manage SST / DST users
  - Create Service Tools User ID (CRTSSTUSR)
  - Change Service Tools User ID (CHGSSTUSR)
  - Delete Service Tools User ID (DLTSSTUSR)

IBM i user profile must have *SECADM and *SERVICE special authority and Service Tool user functional privilege "Service Tools Security" to be able to call this CL command



```
                      Create Service Tool

Type choices, press Enter.

Requesting SST user ID . . . . .   barlen        Character value
Requesting SST user ID pwd . . .
Service tools user ID  . . . . .   jdoe          Character value
Service tools user ID info:
  Password . . . . . . . . . . .   K123JJ7662ca
  Status . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED
  Set password to expired  . . .   *yes          *NO, *YES
  Text 'description' . . . . . .   Mr. John Doe
```

Auditing Enhancements

7.4

- DS audit journal type contains now 4 additional entry types
  - D - Delete of a service tools user ID using the DLTSSTUSR command
  - H - Change to a service tools user ID using the CHGSSTUSR command
  - R - Create of a service tools user ID using the CRTSSTUSR command
  - S - Change to the service tools security attributes using the CHGSSTSECA command.

- New DB2 Mirror for i audit journal entry types activated via *SYSMGT audit event class in QAUDLVL/QAUDLVL2 system value
  - M0 - Db2 Mirror setup tools
  - M6 - Db2 Mirror Communication Services
  - M7 - Db2 Mirror Replication Services
  - M8 - Db2 Mirror Product Service
  - M9 - Db2 Mirror Replication Stat

Crypto Performance

- Power 8/9 in-core Cryptographic Performance Acceleration
  - Support within the processor itself, no additional products or HW required
  - *Automatic* performance acceleration for certain cryptographic algorithms
    - AES & SHA-2 message digest
  - Does not support “cryptographic key” storage
    - Certain customers will still need the HW Cryptographic Coprocessor Card
  - Performance gains will be realized in support such as:
    - Customer applications that use the Cryptographic Services APIs
    - SSL (Secure Socket Layer) / Transport Layer Security (TLS)
    - VPN (Virtual Private Network)
    - Software Tape Encryption

Agenda

- Base IBM i security enhancements
- Access Control security enhancements
- Database security enhancements
- Network security enhancements

IBM i Authority Collection

Background: Security and Compliance - The Issue

- Customers run many applications on a single partition
  - No detailed knowledge of the applications… where is the data?
    - Data in DB2 or IFS … but where?
  - Once found, how do you lock down security without application breakage?
    - What is the “minimum” authority level that can be granted for the end user?
  - Many customers have little to no idea what interfaces an application uses so the authority requirements cannot be determined
  - Applications are shipped with excessive public authority (common problem) which leads to security exposures
- The problem: customers don’t change security leaving data exposed

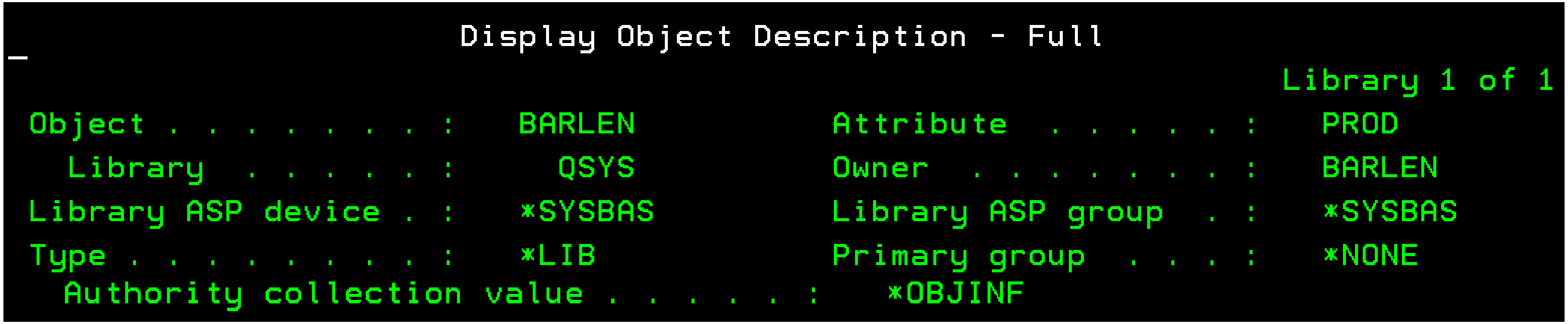
Solution: IBM i Authority Collection

- Initially introduced with IBM i V7.3
- Utility that captures pertinent data associated with an authority check
  - Included as part of the base IBM i OS
  - The collection covers all native IBM i file systems
  - Focus on capturing only unique instances of the authority check
  - Run-time performance, while the collection is active, will degrade 2-3%
  - Storage consideration for long running authority collection
- The collection includes key pieces of information… (including)

What authority is required for this authority check

Implementation

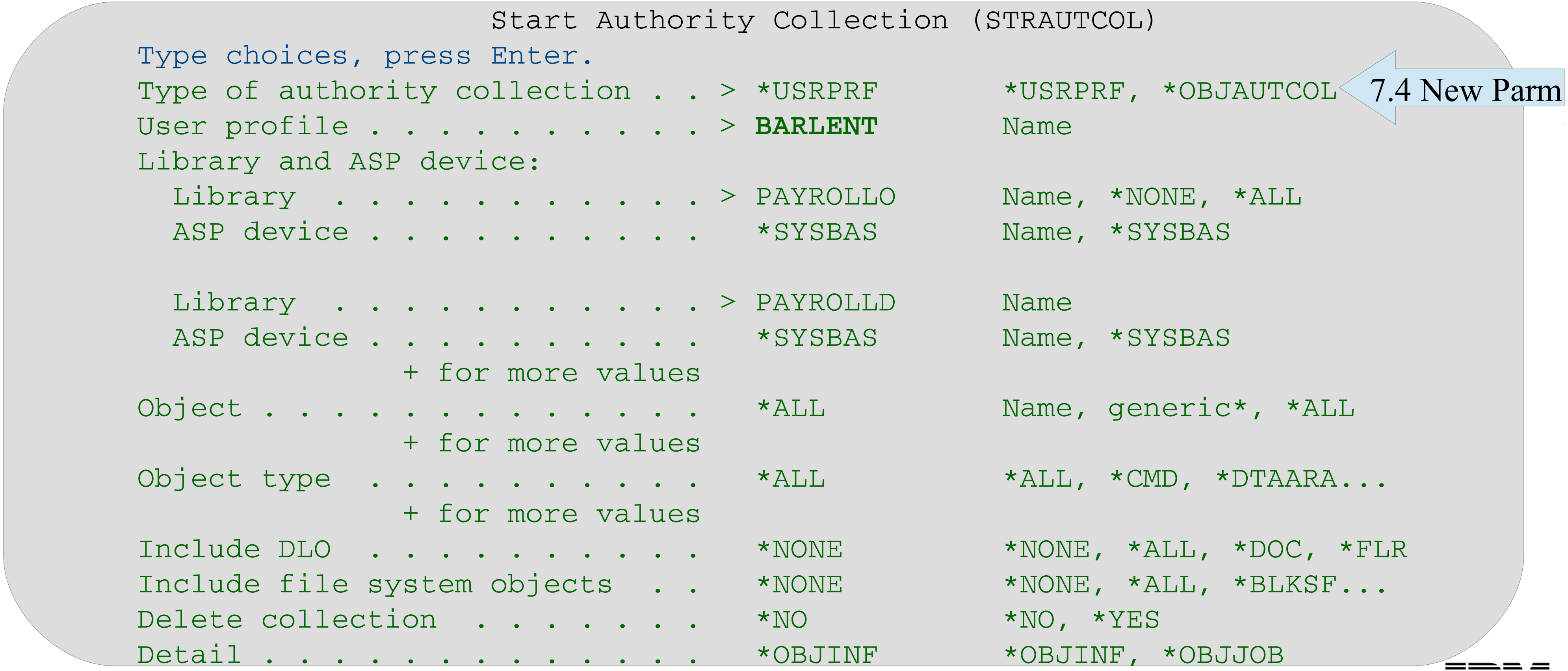
- The Authority collection is “user” based in the 7.3 release
  - Turn on the authority collection for a given user(s)
  - Collect authority information for the user
    - Cannot collect information on the group level but object access allowed via a group profile authority is collected
    - Adopted authority information collected
- Authority collection can now be enabled on an object basis 7.4
  - Collect information for a given object
  - New attribute on every object specifies whether authority collection is enabled



```
                        Display Object Description - Full
_
                                                                  Library 1 of 1
 Object . . . . . . . . :    BARLEN           Attribute . . . . . :    PROD
   Library  . . . . . . :      QSYS           Owner . . . . . . . :    BARLEN
 Library ASP device . . :    *SYSBAS          Library ASP group . :    *SYSBAS
 Type . . . . . . . . . :    *LIB             Primary group . . . :    *NONE
   Authority collection value . . . . . . :    *OBJINF
```

Running the collection – Start collection for user(s)

- Collection is started with the Start Authority Collection (STRAUTCOL) command
  - Requires at least the user profile to be specified and a library selection



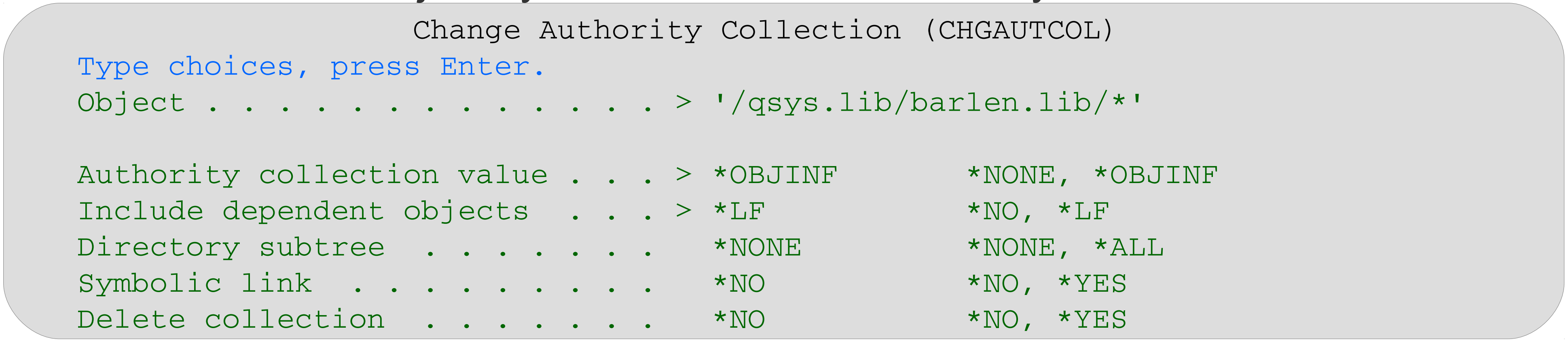
```
                    Start Authority Collection (STRAUTCOL)
Type choices, press Enter.
Type of authority collection . . > *USRPRF        *USRPRF, *OBJAUTCOL
User profile . . . . . . . . . . > BARLENT        Name
Library and ASP device:
  Library  . . . . . . . . . . . > PAYROLLO       Name, *NONE, *ALL
  ASP device . . . . . . . . . .   *SYSBAS        Name, *SYSBAS

  Library  . . . . . . . . . . . > PAYROLLD       Name
  ASP device . . . . . . . . . .   *SYSBAS        Name, *SYSBAS
               + for more values
Object . . . . . . . . . . . . .   *ALL           Name, generic*, *ALL
               + for more values
Object type  . . . . . . . . . .   *ALL           *ALL, *CMD, *DTAARA...
               + for more values
Include DLO  . . . . . . . . . .   *NONE          *NONE, *ALL, *DOC, *FLR
Include file system objects  . .   *NONE          *NONE, *ALL, *BLKSF...
Delete collection  . . . . . . .   *NO            *NO, *YES
Detail . . . . . . . . . . . . .   *OBJINF        *OBJINF, *OBJJOB
```

7.4 New Parm

Running the collection – Start collection for object(s)

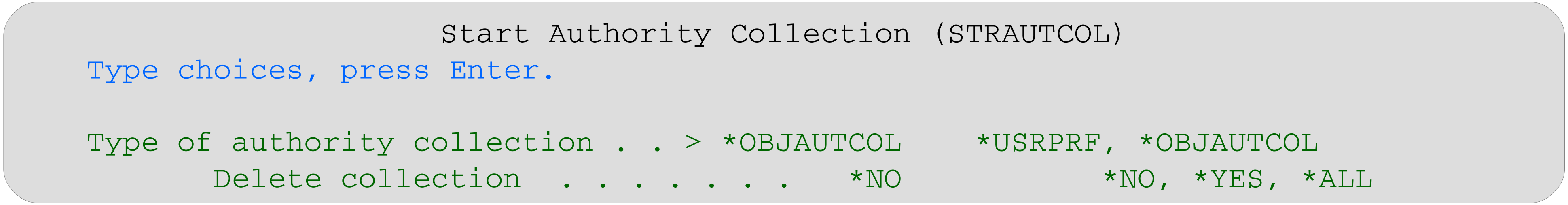
7.4

- Authority collection for objects need to be started differently
  - First define the objects you want to collect authority information for



```
                         Change Authority Collection (CHGAUTCOL)
    Type choices, press Enter.
    Object . . . . . . . . . . . . . > '/qsys.lib/barlen.lib/*'

    Authority collection value . . . > *OBJINF         *NONE, *OBJINF
    Include dependent objects  . . . > *LF             *NO, *LF
    Directory subtree  . . . . . . .   *NONE           *NONE, *ALL
    Symbolic link  . . . . . . . . .   *NO             *NO, *YES
    Delete collection  . . . . . . .   *NO             *NO, *YES
```

  - Next start the collection



```
                         Start Authority Collection (STRAUTCOL)
    Type choices, press Enter.

    Type of authority collection . . > *OBJAUTCOL    *USRPRF, *OBJAUTCOL
           Delete collection  . . . . . . .   *NO           *NO, *YES, *ALL
```

Running the collection - Stop

7.4

- Collection is ended with the End Authority Collection (ENDAUTCOL) command
  - Ending user-based collection:

```
                    End Authority Collection (ENDAUTCOL)

 Type choices, press Enter.
 Type of authority collection . .   *USRPRF        *USRPRF, *OBJAUTCOL
 User profile . . . . . . . . . .   BARLENT        Name
```

7.4 New Parm

  - Ending object-based collection:

```
                    End Authority Collection (ENDAUTCOL)

 Type choices, press Enter.
 Type of authority collection . .   *OBJAUTCOL   *USRPRF, *OBJAUTCOL
```

Determine list of objects with enabled collection

7.4

QSYS

- It is not obvious which objects have turned on the authority collection attribute
- The following SQL statement can be used to list all object where the authority collection value has been set to *OBJINF
  - Note → this command can take a while to complete
    - It is better to remember what you have activated

```
SELECT * FROM TABLE (QSYS2.OBJECT_STATISTICS('*ALLUSR ','*ALL') ) AS X
WHERE AUTHORITY_COLLECTION_VALUE = '*OBJINF'
```

```
OBJNAME      OBJTYPE    OBJOWNER     OBJDEFINER   OBJCREATED
STARTSYSBK   *PGM       BARLEN       BARLEN       2017-09-29-07.12.24.000000
STARTSYSL    *PGM       BARLEN       SXHANSON     2017-10-23-10.32.38.000000
SYSLOG1      *PGM       BARLEN       BARLEN       2017-08-09-11.53.48.000000
SYSLOG2      *PGM       BARLEN       BARLEN       2017-08-09-11.56.02.000000
SYSLOG3      *PGM       SPHANSON     SXHANSON     2017-11-02-11.19.13.000000
SYSLOG3S     *PGM       BARLEN       BARLEN       2019-04-26-10.50.24.000000
```

Determine list of objects with enabled collection

7.4

IFS

- The following command and SQL statement can be used to list all object where the authority collection value has been set to *OBJINF for a given IFS directory

```
RTVDIRINF DIR(/) OMIT('/QSYS.LIB')
```

This will produce a QAEZDxxxxO file

- List the objects with the authority collection value set to *OBJINF

```
SELECT QEZOBJNAM, QEZOBJTYPE, QEZAUTCOL FROM QUSRSYS.QAEZDxxxxO
  WHERE QEZAUTCOL = '*OBJINF'
```

Check for active authority collections for users

- The following command and SQL statement can be used to check the status of user-based authority collections

```
  SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
    QSYS2.USER_INFO WHERE
```

```
AUTHORIZATION_NAME  AUTHORITY_COLLECTION
                    _ACTIVE
    SECHARD                 NO
    SLOPR                   NO
    SSHGRP                  NO
    SYSLOG                  NO
    TBARLEN                 YES
    THOMAS                  NO
    THOMAS2FA               YES
    TOMTEST1                NO
```

- Just checking for active collections

```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
QSYS2.USER_INFO WHERE AUTHORITY_COLLECTION_ACTIVE='YES'
```

Check for existing user collection repositories

- The following command and SQL statement can be used to check the existence of user-based authority collection repositories

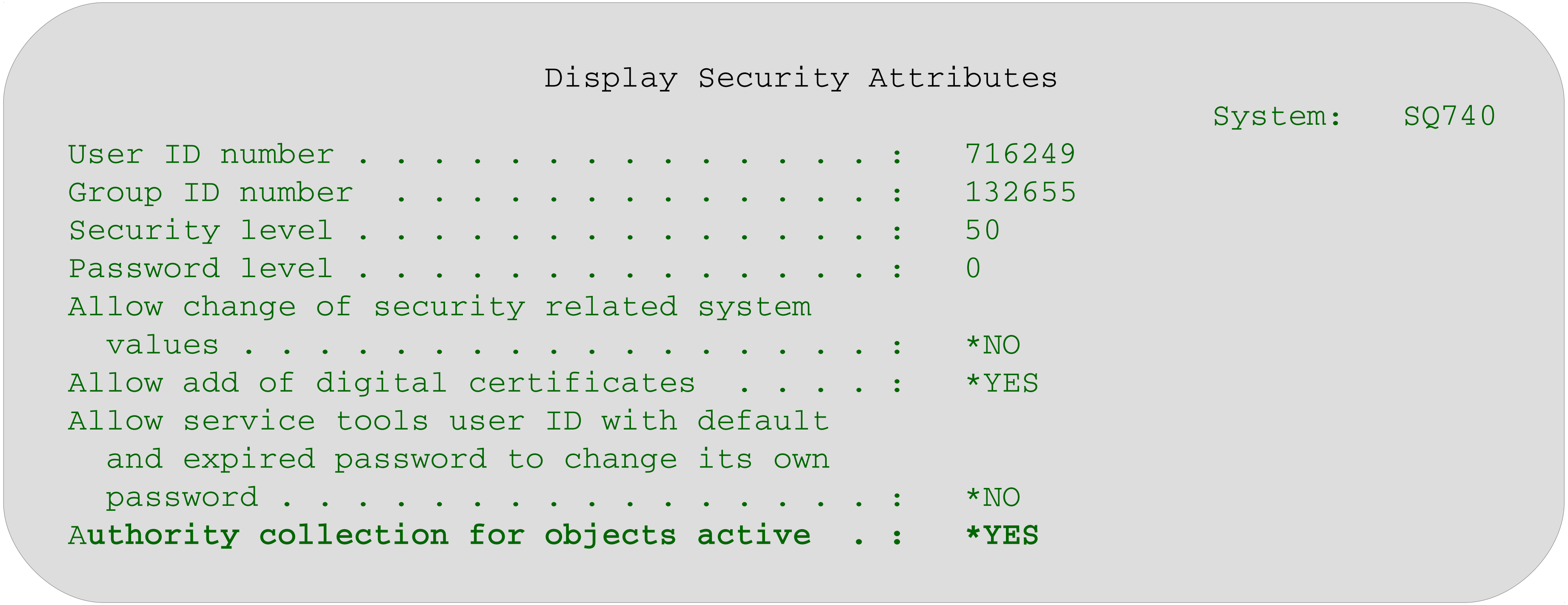
```
SELECT AUTHORIZATION_NAME, AUTHORITY_COLLECTION_ACTIVE FROM
QSYS2.USER_INFO WHERE AUTHORITY_COLLECTION_REPOSITORY_EXISTS='YES'
```

```
AUTHORIZATION_NAME  AUTHORITY_COLLECTION
                    _ACTIVE
    BARLEN                  NO
    THOMAS2FA               YES
```

Check for active authority collections for objects

7.4

- The Display Security Attributes (DSPSEAC) command can be used to check if object-based authority collection has been started on the system



```
                        Display Security Attributes
                                                       System:   SQ740
User ID number . . . . . . . . . . . . . . . :   716249
Group ID number  . . . . . . . . . . . . . . :   132655
Security level . . . . . . . . . . . . . . . :   50
Password level . . . . . . . . . . . . . . . :   0
Allow change of security related system
  values . . . . . . . . . . . . . . . . . . :   *NO
Allow add of digital certificates  . . . . . :   *YES
Allow service tools user ID with default
  and expired password to change its own
  password . . . . . . . . . . . . . . . . . :   *NO
Authority collection for objects active  . . :   *YES
```

Captured data analysis

- Collected data is stored in table QSYS2.AUTHORITY_COLLECTION
  - The collected information contains the following:
    - Object name, Library name, ASP device, Object type
    - SQL name, SQL object type, SQL schema name
    - Path name and object name
    - Authorization list for the object
    - Required authority
    - Current authority
    - Authority source for the user that satisfies the authority request
    - Adopted authority indicator (adopt was used to satisfy the authority request), Current adopted authority, Adopted authority source, Adopting program name and indicator (adopting program that was used to satisfy the authority request), Adopting program library, Adopting program object type (*PGM or *SRVPGM), Adopting program owner
    - Stack info (most recent invocation and most recent user state invocation including procedure name and statement)
    - Job name, Job user, Job number
      - Current job user profile
      - Group profile and indicator (group profile that was used to satisfy the authority request)
  - Date and time of authority check

Captured data analysis (cont'd)

- Example of a query output for a user collection

```
SELECT AUTHORIZATION_NAME,OBJECT_NAME,SYSTEM_OBJECT_TYPE,
DETAILED_REQUIRED_AUTHORITY,
DETAILED_CURRENT_AUTHORITY,AUTHORITY_SOURCE
FROM QSYS2.AUTHORITY_COLLECTION WHERE USER_NAME = 'BARLENT'
```

```
AUTHORIZATION OBJECT_NAME  SYSTEM_ DETAILED_REQUIRED_AUTHORITY        AUTHORITY_SOURCE
_NAME                      OBJECT_
                           TYPE


    BARLENT   SALES          *FILE *OBJOPR                            USER PRIVATE
    BARLENT   SALES          *FILE *OBJOPR *READ                      USER PRIVATE
    BARLENT   SALESPGM       *PGM  *OBJOPR *READ *EXECUTE             PUBLIC
    BARLENT   SALESPGM       *PGM  *OBJOPR                            PUBLIC
```

Captured data analysis (cont'd)

7.4

- Example of a query for an object collection
  - See who performed changes on file SALARIES in library PAYROLL

```
WITH emp_activity (username, cur_auth, req_auth) AS (
        SELECT "CURRENT_USER",
               detailed_current_authority,
               detailed_required_authority
            FROM qsys2.authority_collection_object aco
            WHERE system_object_schema = 'PAYROLL'
                  AND system_object_name = 'SALARIES'
                  AND adopting_program_owner IS NULL
    )
    SELECT *
        FROM emp_activity
        WHERE req_auth LIKE '%UPD%'
              OR req_auth LIKE '%DLT%'
              OR req_auth LIKE '%ADD%';
```

Captured data analysis (cont'd)

7.4

- Following collection objects are available when using object-based authority collections
  - AUTHORITY_COLLECTION_OBJECT
    View to look at information that was collected for libraries and objects in libraries during authority collection for objects.
  - AUTHORITY_COLLECTION_LIBRARIES
    View to look at information that was collected for all libraries and objects in libraries during authority collection for objects.
    - QSYS2.AUTHORITY_COLLECTION_OBJECT and QSYS2.AUTHORITY_COLLECTION_LIBRARIES return the same results
    - QSYS2.AUTHORITY_COLLECTION_OBJECT will perform better when the number of entries in the authority collection is large and you are looking for a specific object
    - QSYS2.AUTHORITY_COLLECTION_LIBRARIES will perform better when the number of entries in the authority collection is small or you are looking for all or most objects in the authority collection

Captured data analysis (cont'd)

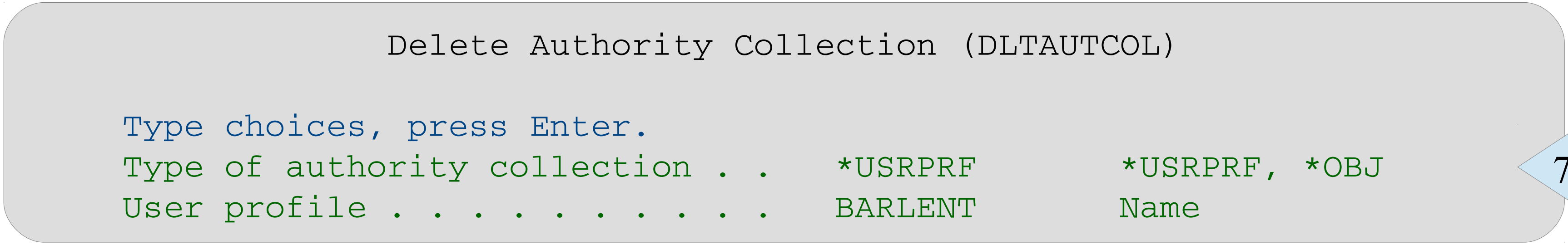
7.4

- AUTHORITY_COLLECTION_FSOBJ
  View to look at information that was collected for all file system objects in the "root" (/), QOpenSys, and user-defined file systems
- AUTHORITY_COLLECTION_DLO
  View to look at information that was collected for document library objects (DLO)

Deleting the collection

7.4

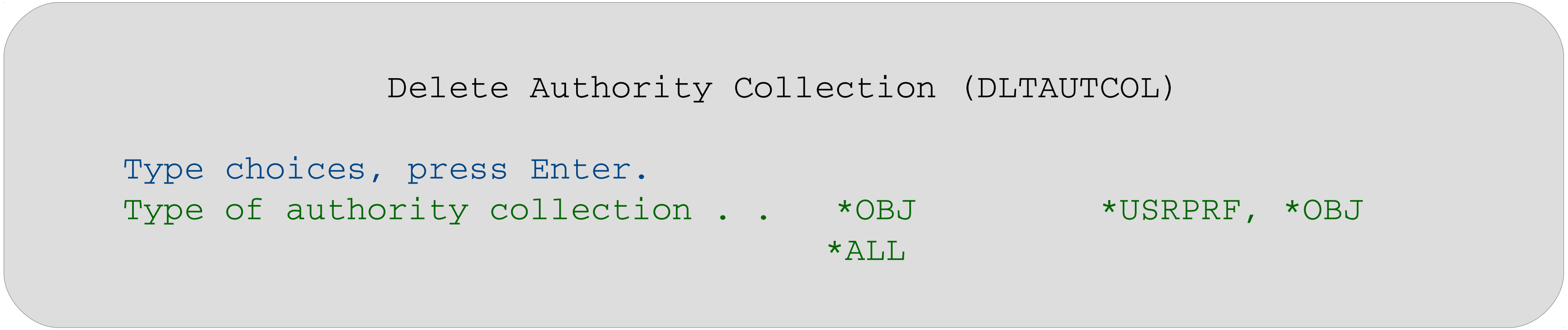
- The authority collection can be deleted with the Delete Authority Collection (DLTAUTCOL) command
  - Ending user-based collection:



```
                    Delete Authority Collection (DLTAUTCOL)

     Type choices, press Enter.
     Type of authority collection . .   *USRPRF       *USRPRF, *OBJ
     User profile . . . . . . . . . .   BARLENT       Name
```

7.4 New Parm

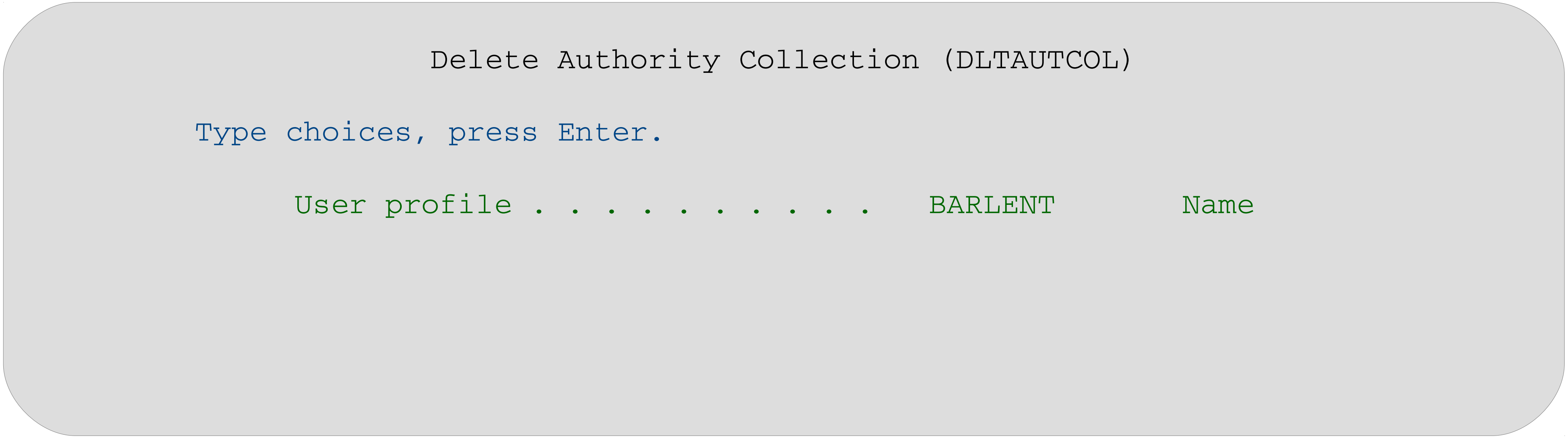
  - Ending object-based collection:



```
                    Delete Authority Collection (DLTAUTCOL)

     Type choices, press Enter.
     Type of authority collection . .   *OBJ          *USRPRF, *OBJ
                                       *ALL
```

Deleting the collection

- The authority collection is for a given user is deleted with the Delete Authority Collection (DLTAUTCOL) command
  - Requires at only the user profile to be specified



```
                 Delete Authority Collection (DLTAUTCOL)

 Type choices, press Enter.

     User profile . . . . . . . . . .   BARLENT       Name
```

Agenda

- Base IBM i security enhancements
- Access Control security enhancements
- Database security enhancements
- Network security enhancements

Database Security Enhancements

- Business data is one of the most valuable assets in a company
- Sensitive data must be properly protected
  - Access control via object permissions
  - Encryption of sensitive data
  - Monitoring of unauthorized access attempts
  - Monitoring and control of read / write access over the network
  - Classification of data
- Most protection measures have been in IBM i for many years
- DB2 for IBM i provides new functions that can be used to implement
  - More granular access controls
  - Transparent encryption of data

Database Encryption

- IBM i provides several methods for encrypting data at rest
  - Common Cryptographic Architecture (CCA) APIs that use the 4765 / 4767 cryptographic coprocessor
  - Cryptographic Services APIs
  - SQL encryption
- Using APIs to encrypt data within the business application requires changes to
  - Application code
  - Database column types and length
  - Interface changes for importing and exporting data
- New functions can be used to
  - Provide transparent encryption to applications
  - Data masking
  - Access control to data

7.1 IBM i DB2 Field Procedures

Column Level Encryption and Data Masking Enablement

DB2 Field Procedures – 7.1

- **DB2 Column Level (field) exit support**
  - Exit program (Field Procedure) called on insert/update/read of a column
  - Similar to “Triggers” but additional support to enable encryption
  - Exit added via SQL Alter Table
    - One exit per column

- **Enables Column Level Encryption**
  - Encrypt/Decrypt data in a DB2 column
    - No need to change column attributes like field length or data type
  - Encryption Key management must be implemented by the Exit Program (Field Procedure)

DB2 Field Procedures – 7.1

- **Data Masking support**
  - Depending on FieldProc controls, data can be masked during decoding
  - Example: User might just see last 4 digits of credit card PAN
    PAN: **** **** **** 1233
  - Special considerations when updating or inserting rows
    - Special return code specified in sqlstate parameter Field Encoding function

DB2 handles all length and data type issues

- I/O buffer doesn't change but encrypted data length and data type can change
  - I/O buffer for SS# is 9 and type character
  - Result of encryption is, for example, length 16 and data type binary
    - Managed by DB2 internally

- **Field Procedure is a user written program**
  - Business partner solutions are available as well
    Example: Syncsort(Enforcive/Vision Solutions), Raz-Lee, Patrick Townsend, Linoma

Row and Column Access Control

Row and Column Access Control (RCAC) - 7.2

- Provides more granular access control to columns or rows depending on user/group
- Implemented in DB
- Controls access for all interfaces, i.e. native SQL, ODBC, FTP, etc.
- Two sets of rules
  - Row access
    - Returns only rows where a user has access to
  - Column access
    - Masks data that a user does not has access to
- *IBM Advanced Data Security for i* is required
  - No-charge feature, IBM i Option 47 required for RCAC

Implementation

- RCAC can be used to complement the table privileges model
- Implemented via SQL commands
- Alters a table and adds access controls for rows and columns
- Enforced via database engine

Custno	Name	City	Country	Revenue
33123	Star hotels	Mainz	DE	*******
44541	Super hotels	Athens	GR	*******
45211	Bakery No 1	London	GB	32223.33
66541	Golden Pub	Manchester	GB	787611.32
76112	BBQ Joint	Raleigh	US	*******

Row access control

- Limit access to rows based on accessing user or group membership

```
CREATE PERMISSION SALARY_ROW_ACCESS ON EMPLOYEE
   FOR ROWS WHERE VERIFY_GROUP_FOR_USER(SESSION_USER,
         'MGRGRP') = 1
   ENFORCED FOR ALL ACCESS
   ENABLE;

COMMIT;
ALTER TABLE EMPLOYEE
ACTIVATE ROW ACCESS CONTROL;
COMMIT;
```

```
SESSION_USER: Current job user
CURRENT_USER: Most recent adopted user
              When no adopted authority is
              active, the effective user
              of the thread Is returned.
SYSTEM_USER: The authorization ID that
              initiated the connection
              is returned.
```

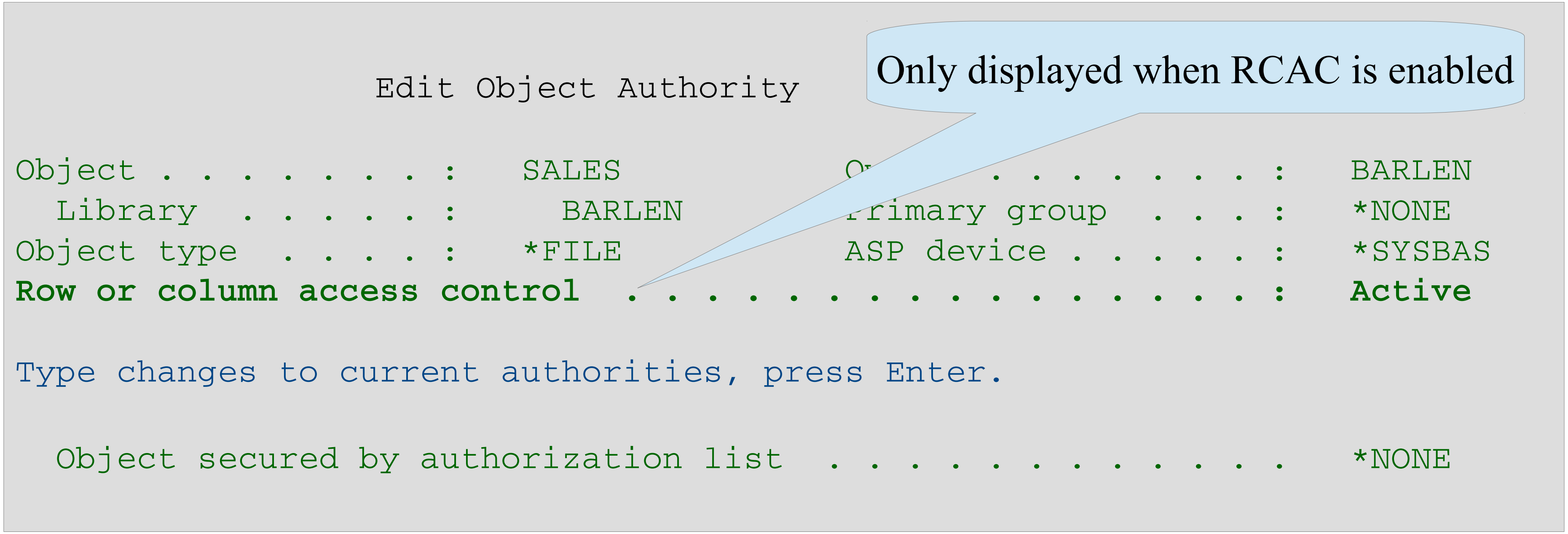
Column access control

- Mask column values for users who do not have access

```
CREATE MASK SSN_MASK ON EMPLOYEE
   FOR COLUMN SSN RETURN
      CASE
       WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER,'PAYROLL') = 1)
            THEN SSN
       WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER,'MGR') = 1)
            THEN 'XXX-XX-' || SUBSTR(SSN,8,4)
         ELSE NULL
      END
   ENABLE;
COMMIT;
ALTER TABLE EMPLOYEE
   ACTIVATE COLUMN ACCESS CONTROL;
COMMIT;
```

Determine if RCAC is enabled for a file

- Display object authority (DSPOBJAUT) provides an easy way to determine if RCAC is enabled for a file



Only displayed when RCAC is enabled

```
                  Edit Object Authority

Object . . . . . . . :    SALES               Owner . . . . . . . :    BARLEN
  Library  . . . . . :      BARLEN            Primary group  . . . :   *NONE
Object type  . . . . :    *FILE               ASP device . . . . . :   *SYSBAS
Row or column access control  . . . . . . . . . . . . . . . . :   Active

Type changes to current authorities, press Enter.

  Object secured by authorization list . . . . . . . . . . . .     *NONE
```

DB2 for i RCAC Redpaper

Many of your RCAC questions will be answered by reading this Redpaper

IBM

Row and Column Access Control Support in IBM DB2 for i

Implement roles and separation of duties

Leverage row permissions on the database

Protect columns by defining column masks

Jim Bainbridge
Hernando Bedoya
Rob Bestgen
Mike Cain
Dan Cruikshank
Jim Denton
Doug Mack
Tom McKinley
Kent Milligan

ibm.com/redbooks

Redpaper

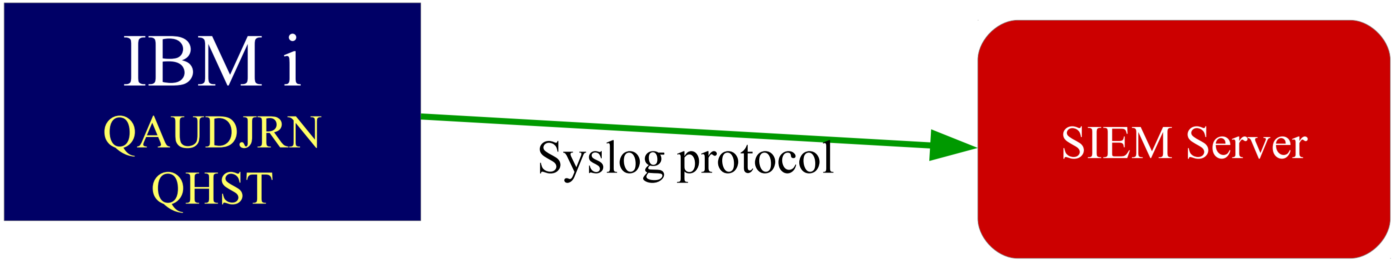
www.redbooks.ibm.com/redpieces/abstracts/redp5110.html

Agenda

- Base IBM i security enhancements
- Access Control security enhancements
- Database security enhancements
- Network security enhancements

Syslog reporting

- Demand for reporting security information to central Security Information and Event Management (SIEM) systems (i.e. QRADAR, SPLUNK, ArcSight)
- DB2 group PTF levels for IBM i 7.2 (SF99702) and 7.3 (SF99703) introduce syslog format support
- DB2 table functions DISPLAY_JOURNAL and HISTORY_LOG_INFO have been extended
  - New GENERATE_SYSLOG and EOF_DELAY options



Syslog reporting (cont’d)

- GENERATE_SYSLOG
  - Can format messages according to a standardized format
    - Common Event Format (CEF)
    - Supports format of RFC3164 and RFC5424
- EOF_DELAY
  - Number of seconds of delay before trying to read additional audit journal / history entries when end of file is reached

Example

```
    SELECT syslog_facility, syslog_severity,
    cast(syslog_event as varchar(2048) CCSID 37) FROM TABLE
    (QSYS2.DISPLAY_JOURNAL('QSYS', 'QAUDJRN',
     GENERATE_SYSLOG =>'RFC5424', EOF_DELAY => 10
     ) ) AS X WHERE syslog_event IS NOT NULL AND
     JOURNAL_ENTRY_TYPE IN ('AD','AF','CA','CD','CP','CO','DO',
                'OW','PW','SV');
```

Syslog reporting (cont’d)

- Generated output example

Output example

```
CEF:0|IBM|IBM i|7.3|QSYS-QAUDJRN|T-PW|Low|reason=Invalid password
  msg=User FAKEUSER name not valid suser=QUSER
  sproc=172387/QUSER/QZSOSIGN shost=SQ740 src=127.0.0.1 spt=56903

CEF:0|IBM|IBM i|7.3|QSYS-QAUDJRN|T-AF|Medium|reason=Authority failure
  msg=Not authorized to object fileType=*USRPRF
  cs1Label=objName cs1=QSYS/JDPWRSYS suser=JAVA
  sproc=183687/QUSER/QZRCSRVS shost=SQ740
  src=127.0.0.1 spt=43909
```

- Generated CEF formatted messages must still be forwarded via syslog
  - Example: PASE `logger` tool or PASE `syslog()` function
  - Or by using alternative tools → see session Integrating IBM i into Security Information and Event Management (SIEM) systems - i100850
- Information is available from: https://www.ibm.com/developerworks/ibmi/techupdates/db2/groupptf

Transport Layer Security (TLS) 1.3 Support

7.4

- Base IBM i network encryption supports now TLS version 1.3
  - Used by default
    - QSSLPCL default is *TLSV1.3 and *TLSV1.2
  - TLSV1 and TLSV1.1 have been disabled
- SSLv2 has been completely removed from the OS and cannot be activated anymore
- TLS 1.3 is not compatible to previous TLS versions
  - New protocol enhancements include
    - All handshake messages after the Server Hello message are now encrypted
    - SHA and MD5 algorithms completely removed
    - Legacy symmetric algorithms have been removed
    - Faster session establishments with features, such as
      - TLS false start
      - Allows a client to already send encrypted data immediately after first TLS roundtrip
      - Reduces the round trip time (RTT) with TLS from 2 to 1
    - TLS fast open (defined in RFC 7413)
      - Defines new TCP option → Fast Open Cookie

Transport Layer Security (TLS) 1.3 Support (cont'd)

7.4

- The default cipher suite list has been significantly reduced in 7.4
  - AES_128_GCM_SHA256
  - AES_256_GCM_SHA384
  - CHACHA20_POLY1305_SHA256

  TLS V1.3 ciphers

  - ECDHE_ECDSA_AES_128_GCM_SHA256
  - ECDHE_ECDSA_AES_256_GCM_SHA384
  - ECDHE_RSA_AES_128_GCM_SHA256
  - ECDHE_RSA_AES_256_GCM_SHA384

  TLS V1.2 ciphers

- CHACHA20 is a stream cipher algorithm
  - Performs better on devices without AES hardware acceleration, i.e. smart phones or tablets

More TLS changes

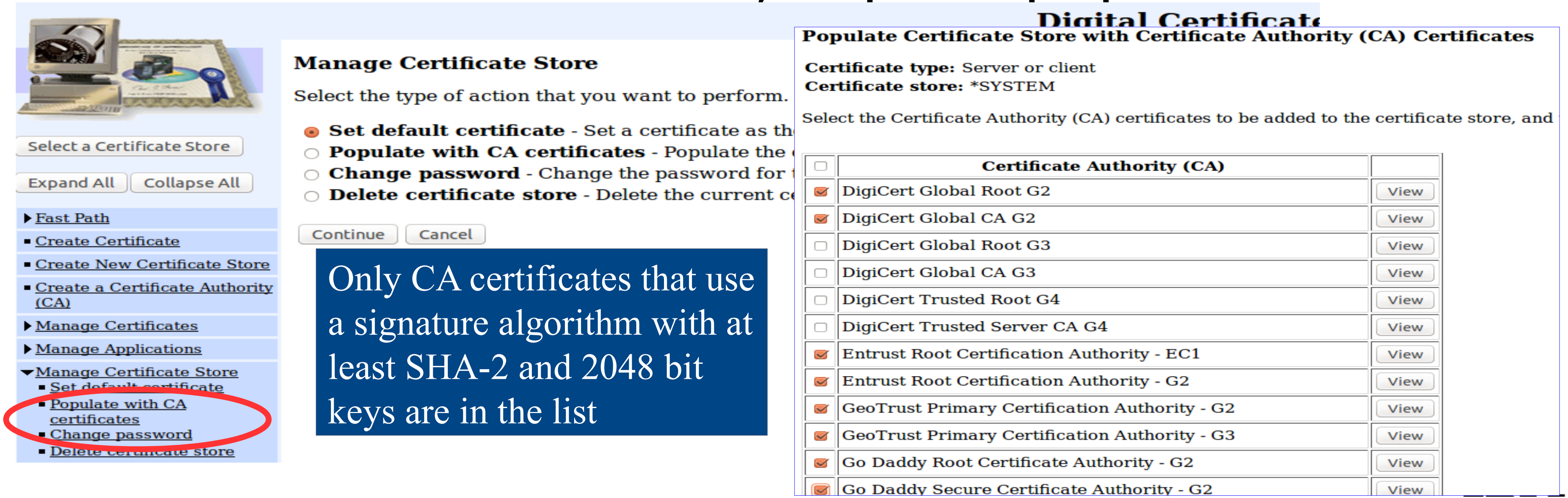
7.4

- In case of network devices, such as proxy servers, that do not support TLS version 1.3, IBM i 7.4 also supports Middlebox compatibility mode
  - Middlebox Compatibility Mode makes the TLS version 1.3 handshake flow look more like a TLS version 1.2 handshake
  - This is accomplished by filling in legacy fields in handshake messages and by sending a TLS version 1.2 handshake message eliminated from the pure TLS version 1.3 implementation
  - System TLS does not initiate middlebox compatibility mode by default. If needed in your network, this mode can be turned on globally for System TLS using TLSCONFIG option middleboxCompatibilityMode
- All references to Secure Sockets Layer (SSL) have been removed and renamed to Transport Layer Security (TLS)
- New API Retrieve TLS Attributes (QsoRtvTLSA) API allows the retrieval of the system-wide System TLS current default properties.
- The properties can be changed and viewed with TLSCONFIG SST macro
  - Formerly named SSLCONFIG macro

7.3 DCM CA Changes

With IBM i 7.3 certificate stores are not preconfigured with trusted CA list

- If CA trust list is needed, explicit population is



Manage Certificate Store

Select the type of action that you want to perform.

● **Set default certificate** - Set a certificate as th
○ **Populate with CA certificates** - Populate the
○ **Change password** - Change the password for
○ **Delete certificate store** - Delete the current ce

Only CA certificates that use a signature algorithm with at least SHA-2 and 2048 bit keys are in the list

Populate Certificate Store with Certificate Authority (CA) Certificates

Certificate type: Server or client
Certificate store: *SYSTEM

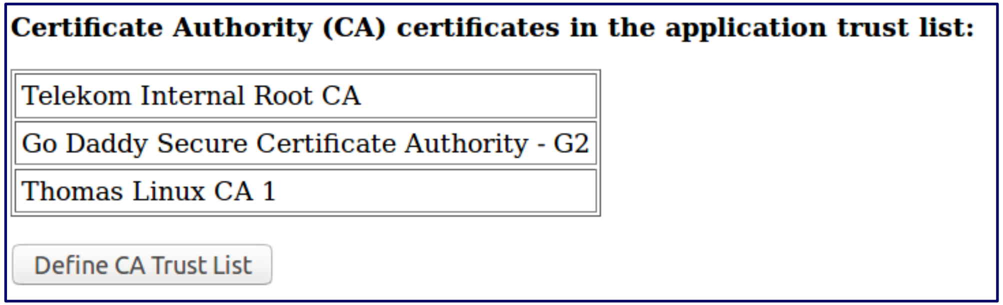
Select the Certificate Authority (CA) certificates to be added to the certificate store, and

☐	Certificate Authority (CA)	
☑	DigiCert Global Root G2	View
☑	DigiCert Global CA G2	View
☐	DigiCert Global Root G3	View
☐	DigiCert Global CA G3	View
☐	DigiCert Trusted Root G4	View
☐	DigiCert Trusted Server CA G4	View
☑	Entrust Root Certification Authority - EC1	View
☑	Entrust Root Certification Authority - G2	View
☑	GeoTrust Primary Certification Authority - G2	View
☑	GeoTrust Primary Certification Authority - G3	View
☑	Go Daddy Root Certificate Authority - G2	View
☑	Go Daddy Secure Certificate Authority - G2	View

Digital Certificate Manager APIs

7.4

- A whole set of new APIs have been introduced to manage certificates via custom programs



Certificate Authority (CA) certificates in the application trust list:

Telekom Internal Root CA
Go Daddy Secure Certificate Authority - G2
Thomas Linux CA 1

Managing Certificate Trust for an application

Add CA Certificate Trust (QycdAddCACertTrust) API

API adds a trusted certificate authority (CA) certificate to the list of trusted CA certificates for an application

Check CA Certificate Trust (QycdCheckCACertTrust) API

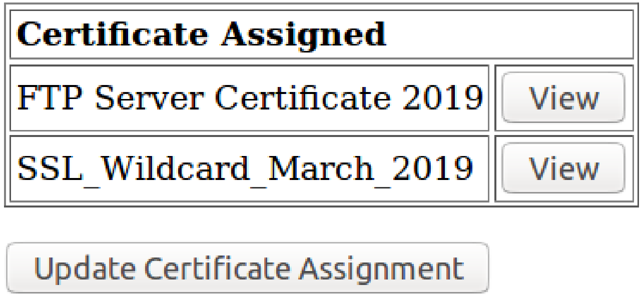
API verifies that the certificate authority (CA) certificates, identified by the list of labels, are trusted by the application

Remove CA Certificate Trust (QycdRemoveCACertTrust) API

API removes a trusted certificate authority (CA) certificate from the list of trusted CA certificates for an application

Digital Certificate Manager APIs (cont'd)

7.4



Certificate Assigned	
FTP Server Certificate 2019	View
SSL_Wildcard_March_2019	View

Managing Certificate Assignment

Update Certificate Usage (QycdUpdateCertUsage) API

API updates the certificate that is assigned to the registered application in the *SYSTEM or *OBJECTSIGNING certificate store. Caller must have *ALLOBJ and *SECADM special authorities

Remove Certificate Usage (QycdRemoveCertUsage) API

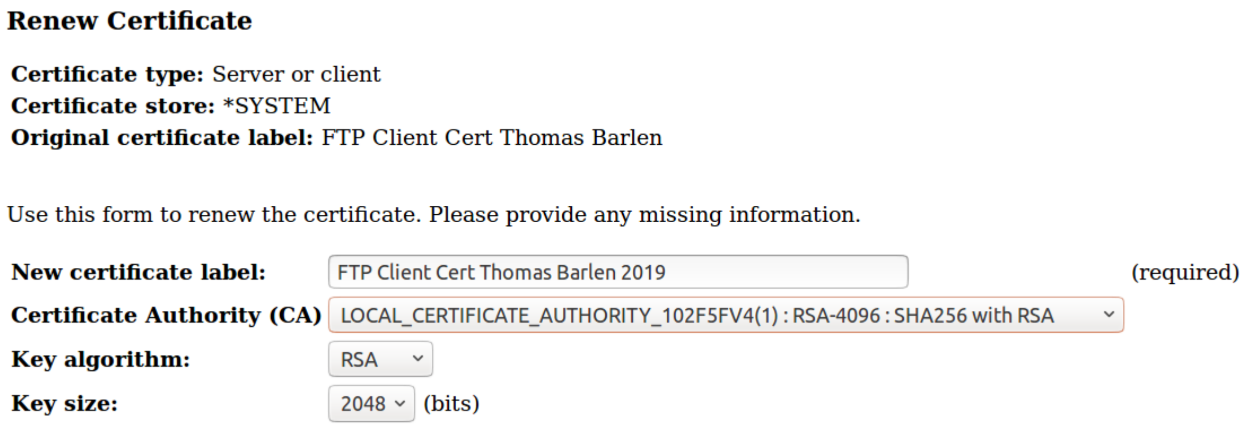
API removes usage of a certificate from a registered application in the *SYSTEM or *OBJECTSIGNING certificate store. Caller must have *ALLOBJ and *SECADM special authorities

Retrieve Certificate Usage Information (QycdRetrieveCertUsageInfo) API

API retrieves information about one or more registered applications that use certificates and their associated certificate information.

Digital Certificate Manager APIs (cont'd)

7.4



Renew Certificate

Certificate type: Server or client
Certificate store: *SYSTEM
Original certificate label: FTP Client Cert Thomas Barlen

Use this form to renew the certificate. Please provide any missing information.

New certificate label:	FTP Client Cert Thomas Barlen 2019	(required)
Certificate Authority (CA)	LOCAL_CERTIFICATE_AUTHORITY_102F5FV4(1) : RSA-4096 : SHA256 with RSA	
Key algorithm:	RSA	
Key size:	2048 (bits)	

Renewing Certificates

Renew Certificate (QycdRenewCertificate) API

API helps to automate the renew certificate process by creating and returning a CSR (Certificate Signing Request) based on an existing certificate and importing an issued certificate into the system certificate store.

The API is called twice in the renewal process:

1. Request a new public/private key pair and receive a certificate signing request based on an expiring certificate
2. After the CSR has been sent to a CA and an issued certificate has been received, the API is called a second time to have the newly issued certificate imported into the system certificate store

FTP changes

7.4

- FTP is passive mode caused problems in the past
  - Data ports in the range of 1024 – 65535 were dynamically assigned
  - Firewall administrators did not like this as it required poking many holes into the firewall
- New environment variable has been introduced to specify a range of ports that are used for passive FTP

```
ADDENVVAR ENVVAR(QIBM_FTP_PORT_RANGE) VALUE('3000-5000') LEVEL(*SYS)
```

  - The range can be between 1 and 65535
  - The FTP server must be restarted after the environment variable has been defined

NetServer changes

7.4

- NetServer and the QNTC file system now support SMB protocol version 3
- End-to-end data encryption for the entire client-server communication
- Support for larger read and write sizes (512 kb)

Networking Enhancements

Kerberos support for single sign-on

- Additional encryption algorithms supported
- RC4-HMAC, AES 128-bit, and AES 256-bit
  - Available via PTFs for V5R4, V6R1, and V7R1
- Steps to utilize new algorithms in an existing environment
  - Remove key table entries from IBM i key table and re-add them
  - Uncheck „DES Only“ option in Active Directory and change service account password
- IBM i Telnet client and FTP server/client have been enabled for SSO → V7R2

Summary

- Use base IBM i security functions
- Protect your database
- Utilize network encryption features to keep data secure while in transit

PowerSC Tools for IBM i

- ü ***Simplifies management*** *and measurement of security & compliance*
- ü ***Reduces cost*** *of security & compliance*
- ü ***Improves detection*** *and reporting of security exposures*
- ü ***Improves*** *the* ***audit capability*** *to satisfy reporting requirements*

IBM Lab Services offerings for IBM i security:

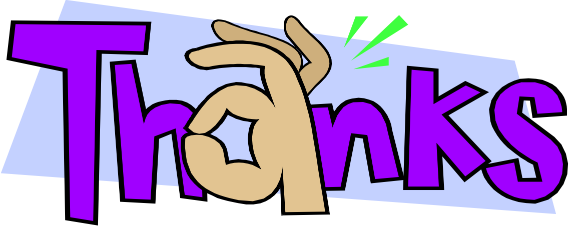
- *IBM i Security Assessment*
- *IBM i Single Sign On Implementation*
- *IBM i Security Remediation*
- *Password Validation, Synchronization, 2FA*
- *IBM i Encryption*

PowerSC Tools for IBM i	Benefits
Compliance Assessment and Reporting	Demonstrate adherence to pre-defined and customer defined security polices, system component inventory. Centralize security management and reporting via Db2 Web Query
Security Diagnostics	Reduces operator time involved in remediating exposures
Privileged Access Control	Ensures compliance with guidelines on privileged users
Access Control Monitor	Prevents user application failures due to inconsistent controls
Network Interface Firewall	Reduces threat of unauthorized security breach and data loss
Certificate Expiration Manager	Prevents system outages due to expired certificates
Password Validation / Synchronization / TOTP Two Factor Authentication (2FA)	Ensures user passwords are not trivial and are in synchronization across all LPARs. Insure service accounts adhere to policy - including SVRAUTE. Enhance applications with 2FA service program.
Single Sign On (SSO) Suite	Reduces for password resets and simplifies user experience

PowerSC Tools for IBM i is a service offering from IBM Systems Lab Services

For more information on PowerSC Tools for IBM i offerings and services, contact: Terry Ford (taford@us.ibm.com) or Thomas Barlen (barlen@de.ibm.com), IBM Systems Lab Services Security

THANK YOU



Thomas Barlen

Senior Managing Consultant

barlen@de.ibm.com

IBM Systems Lab Services and Training

Our Mission and Profile

- Support the IBM Systems Agenda and accelerate the adoption of new products and solutions
- Maximize performance of our clients' existing IBM systems
- Deliver technical training, conferences, and other services tailored to meet client needs
- Team with IBM Service Providers to optimize the deployment of IBM solutions (GTS, GBS, SWG Lab Services and our IBM Business Partners)

Our Competitive Advantage

- Leverage relationships with the IBM development labs to build deep technical skills and exploit the expertise of our developers
- Combined expertise of Lab Services and the Training for Systems team
- Skills can be deployed worldwide to assure all client needs can be met