TSO/E LOGON:
What Are My Options?
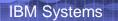

September 16, 2015

Eric Rosenfeld

rosenfel@us.ibm.com

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- z/OS
- RACF

* Registered trademarks of IBM Corporation

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
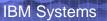
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
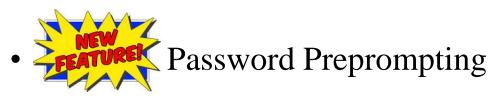
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- In the beginning …
- Exits
- Fullscreen vs. Line Mode
- UADS and RACF Defined Users
- Mixed Case Passwords
- Password Phrases
- VERIFYAPPL
- LOGONHERE
- Password Preprompting

In The Beginning…

- LOGON command
  - Line Mode
  - All parameters needed to be specified
  - Some prompting for values not specified

```
>>__LOGON__user_identity_____>
                        |_/password_____|
                        |_/new_password_|


 >_____>
    |_ACCT(account)_|   |_PROC(procedure_name)_|   |_SIZE(integer)_|


    _NOTICES____    _MAIL____
 >__|_____ __|__|_____|_____>
    |_NONOTICES_|   |_NOMAIL_|     |_PERFORM(value)_|     |_RECONNECT____|
                                                          |_NORECONNECT_|


 >_____>< 
    |_SECLABEL(security_label)_|    |_GROUP(name)_|    |_OIDCARD_|
```

Exits - Possible Uses

- IKJEFLD – pre-prompt
  - Supply or change values that users specify on the LOGON command
  - Supply system attributes and user attributes (UPT, PSCB)
  - Provide your own JCL statements
  - Validate the logon information that users enter
  - Display your own logon panel
  - Prevent a user from logging on to TSO/E

- IKJEFLD1 – pre-prompt (authorized)
  - All IKJEFLD uses
  - Supply the first TSO/E command to be executed in the user's session
  - Supply SYSOUT and job classes for the PSCB
  - Supply the primary and secondary language values

Exits - Possible Uses

- IKJEFLN1 – pre-display
  - Supply information for fields on the logon panel

- IKJEFLN2 – post-display
  - Process fields on the logon panel
  - Validate data on the logon panel
  - Re-prompt for data
  - Display help panels

Exits - Possible Uses …

- IKJEFLD3 – post-prompt
  - Examine the JCL statements
  - Modify the JCL statements
  - Provide additional JCL statements
  - Terminate the LOGON command

- IKJEFLD2 – LOGOFF
  - Clean up storage obtained by the logon exit
  - Control re-logons
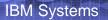 - Gather accounting information

Fullscreen vs. Line Mode

- **Fullscreen**
  - Most prompting done on panel
  - Prefills info from last LOGON

- **Line Mode**
  - All info provided in line mode
  - Only prompted for required data
  - No ability to see last LOGON info

UADS and RACF Defined Users

- UADS
  - Administered by ACCOUNT command/subcommands
  - Can set some authorities
    - JCL, OPER, ACCOUNT, MOUNT, RECOVER

- RACF
  - Administered by RACF ADDUSER/ALTUSER commands
  - TSO segment contains previous LOGON information
  - RACF general resource profiles define access rights
  - Additional fields displayed on LOGON panel (e.g. group, seclabel)
  - Recommended data store
    - Keep emergency IDs in UADS (Revoked in RACF) for disaster recovery

- UADS and RACF
  - Basic info stored in RACF
  - Additional info stored in UADS (e.g. proc, acct)

UADS User

account
 ACCOUNT
list (IBMUSER)
   IBMUSER USER ATTRIBUTES: OPER   ACCT   JCL NOMOUNT   RECOVER
        INSTALLATION ATTRIBUTES, IN HEX: 0000
        MAXSIZE: NOLIM
        USER PROFILE TABLE:
        0038000000000000000000020000001 IBMUSER
        DESTINATION = CENTRAL SITE DEFAULT
        HOLD MSGCLASS= (DEFAULT)
        JOB CLASS   = (DEFAULT)
        MESSAGE CLASS= (DEFAULT)
        SYSOUT CLASS = (DEFAULT)
        NO PERFORMANCE GROUPS
     (*)
      (*)
       IKJACCNT PROCSIZE=   4096K, UNIT NAME= SYSALLDA

RACF User

```
lu ibmuser tso
 USER=IBMUSER  NAME=::::::::::::::::::  OWNER=IBMUSER  CREATED=90.317
 DEFAULT-GROUP=SYS1    PASSDATE=93.056 PASS-INTERVAL=N/A PHRASEDATE=N/A
 ATTRIBUTES=SPECIAL OPERATIONS
 ATTRIBUTES=AUDITOR
 REVOKE DATE=NONE  RESUME DATE=NONE
 LAST-ACCESS=15.221/09:07:18
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)       (TIME)
 ---------------------------------------------
  ANYDAY              ANYTIME
 GROUP=SYS1    AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=93.134
   CONNECTS= 2,505  UACC=READ    LAST-CONNECT=15.221/09:07:18
   CONNECT ATTRIBUTES=NONE
   REVOKE DATE=NONE  RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
 NONE SPECIFIED
 SECURITY-LABEL=SYSMULTI
 DEFINITION OF THIS SECURITY LABEL IS:
  NO INFORMATION IS AVAILABLE
```
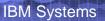
RACF User (cont)

.
.
.

TSO INFORMATION

ACCTNUM= MVS420
PROC= REL5PROC
SIZE= 00050000
MAXSIZE= 00000000
USERDATA= 0000
COMMAND= ispf

User Profile Table (previous LOGON Info) stored, but not listed

RACF Password Options

- SETROPTS (Set RACF Options)

SETR LIST

  .

  .

  .

 PASSWORD PROCESSING OPTIONS:

  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES

  PASSWORD CHANGE INTERVAL IS 30 DAYS.

  PASSWORD MINIMUM CHANGE INTERVAL IS   1 DAYS.

  MIXED CASE PASSWORD SUPPORT IS IN EFFECT

  SPECIAL CHARACTERS ARE ALLOWED.
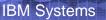
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.

  AFTER   3 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,

    A USERID WILL BE REVOKED.

  PASSWORD EXPIRATION WARNING LEVEL IS   3 DAYS.

  NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.

Mixed Case Passwords

- Enabled by RACF
  - SETROPTS PASSWORD(MIXEDCASE | NOMIXEDCASE)

- TSO/E honors RACF setting
  - Will roll password to upper case if MIXEDCASE not in effect
  - Otherwise will leave as is
  - RACF will allow mixed case password to "match" upper case password in DB until user defines first mixed case password

TSO/E Parmlib

- IKJTSOxx member defines TSO/E attributes

- Set/Modified by:

  – PARMLIB user command

    PARMLIB U(xx)

  – SET console command

    SET IKJTSO=xx

- LOGON statement controls LOGON options

  LOGON PASSPHRASE(ON | OFF)

    VERIFYAPPL(ON | OFF)

    LOGONHERE(ON | OFF)
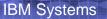
    PASSWORDPREPROMPT(ON | OFF)

Password Phrases

- Enabled via LOGON Statement in IKJTSOxx
  - LOGON PASSPHRASE(ON | OFF)
- Only applies to Fullscreen LOGON
- A password or password phrase can be used
  - Length determines what was used
    - 1-8 Password
    - >8 Phrase
  - In RACF V2R2 a 'Phrase Only' user can be defined
- Panel is modified to allow phrases
- If password expired will re-prompt in same field as password
- To change New Password before expiration select option at bottom of panel
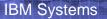
VERIFYAPPL

- Enabled via LOGON Statement in IKJTSOxx
  - LOGON VERIFYAPPL(ON | OFF)

- Passes application ID to RACF when verifying user
- Can restrict access to TSO by APPL class profiles
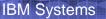- Can implement that only daily statistics be taken when using TSO

LOGONHERE

- Enabled via LOGON Statement in IKJTSOxx
  - LOGON LOGONHERE(ON | OFF)

- Make LOGON RECONNECT work even if the user is not disconnected

- Allows LOGON when **IKJ56411I TSOLOGON RECONNECT REJECTED -USERID userid IN USE** is issued otherwise

Password Preprompting

- Enabled via LOGON Statement in IKJTSOxx
    - LOGON PASSWORDPREPROMPT(ON | OFF)
- Enforces that userid and password entered prior to displaying panel
- Applies to password phrases also
- Will not provide evidence of an existing user if authentication fails
- Ensures that previous logon information is not displayed prior to successful authentication
- Processing occurs after IKJEFLD and IKJEFLD1
    - If other existing exits interrogate/alter Userid or Password in additional processing they may need to be altered before activating
        - Includes RACROUTE REQUEST=VERIFY Exits
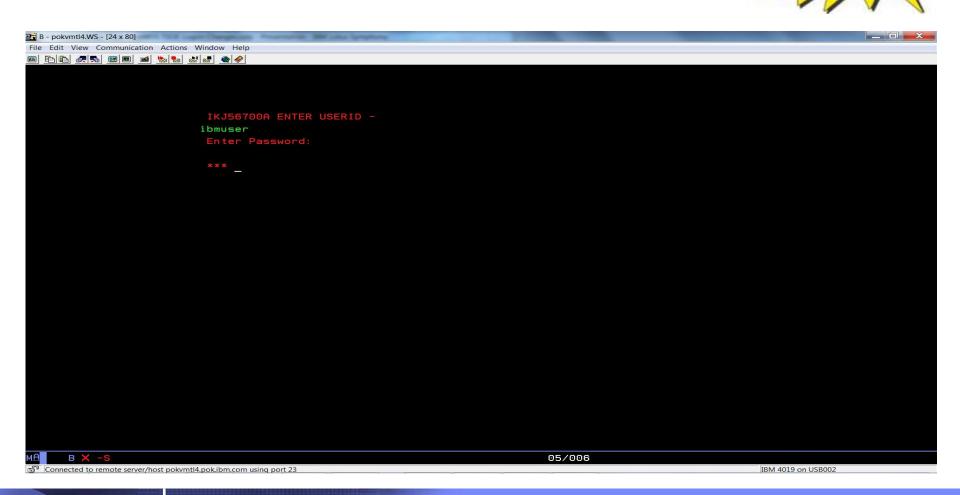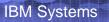- Shipped via PTFs for APAR OA44855 at V1R13, V2R1 and V2R2

Password Preprompting

© 2015 IBM Corporation

Password Preprompting


```
B - pokvmtl4.WS - [24 x 80]
File  Edit  View  Communication  Actions  Window  Help

------------------------------ TSO/E LOGON ------------------------------------


        Enter LOGON parameters below:              RACF LOGON parameters:

        Userid    ===> IBMUSER

                                                   New Password ===>

        Procedure ===> RACFR1A                     Group Ident  ===>

        Acct Nmbr ===>

        Size      ===>

        Perform   ===>

        Command   ===>

        Enter an 'S' before each option desired below:
                    -Nomail          -Nonotice        -Reconnect         -OIDcard

  PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
  You may request specific help information by entering a '?' in any entry field



MA     B                                        10/020
Connected to remote server/host pokvmtl4.pok.ibm.com using port 23          IBM 4019 on USB002
```

Password Preprompting


```
B - pokvmtl4.WS - [24 x 80]
File  Edit  View  Communication  Actions  Window  Help


        Enter Password:

        IKJ56474I  USERID  OR  PASSWORD  IS  INCORRECT  OR  NOT  AUTHORIZED
        ******
      _
```

```
MA      B X SYSTEM                                           05/001
      Connected to remote server/host pokvmtl4.pok.ibm.com using port 23                    IBM 4019 on USB002
```

Where Have We Been?

- In the beginning …
- Exits
- Fullscreen vs. Line Mode
- UADS and RACF Defined Users
- Mixed Case Passwords
- Password Phrases
- VERIFYAPPL
- LOGONHERE
- NEW FEATURE! Password Preprompting

References:
TSO/E Command Reference
TSO/E Customization
TSO/E System Programming Command Reference