

IBM Security zSecure Manager for RACF z/VM
Password Encryption Upgrade to KDFAES

Documentation updates



Contents

- Chapter 1. About this document..... 1**
- Chapter 2. zSecure Manager for RACF z/VM User Reference Manual.....3**
 - Introduction: A sample run..... 3
 - RACF Administration Guide: RA.U USER - User profile detail display..... 4
 - RACF Administration Guide: RA.U USER - Additional selection-Attributes..... 5
 - RACF Audit Guide: SETROPTS - RACF settings report..... 5
 - RACF Audit Guide: SETROPTD - RACF SETROPTS settings in database..... 6
- Chapter 3. zSecure CARLa Command Reference..... 9**
 - SELECT/LIST Fields: RACF..... 9
 - SELECT/LIST Fields: SETROPTS..... 10
 - SELECT/LIST Fields: SYSTEM..... 10
- Chapter 4. zSecure Messages Guide..... 13**

Chapter 1. About this document

Several enhancements were made to RACF to improve the security of passwords and password phrases. The zSecure RACF Password Service Stream Enhancement (SSE) implements changes to zSecure products to correctly process RACF profiles after activation of new RACF functions:

- Allow stronger encryption of passwords
- Accept additional characters within passwords

Other changes did not require documentation updates and are, therefore, not described in the attached PDF file. For example:

- Support in the zSecure MERGE function: uses the appropriate fields for the migration of passwords from the source to the target system.
- Support in the zSecure SMF reporting function: RACF commands can have extra keywords and parameters.

All updates apply to zSecure Manager for RACF® z/VM® version V1.11.1 and some updates also apply to V1.11.2.

This document lists the updates for these enhancements to the following IBM® Security zSecure Manager for RACF z/VM documentation for V1.11.2 and V1.11.1:

IBM Security zSecure Manager for RACF z/VM User Reference Manual, LC27-4364

IBM Security zSecure CARLa Command Reference, LC27-6548

IBM Security zSecure Messages Guide, SC27-6549

Note: Referenced topics that have not changed are not included in this document. You can find them in the publication that the chapter applies to.

Chapter 2. zSecure Manager for RACF z/VM User Reference Manual

This chapter lists the updates for the *IBM Security zSecure Manager for RACF z/VM User Reference Manual* as a result of the RACF password enhancement.

Introduction: A sample run

This update applies to zSecure Manager for RACF z/VM versions V1.11.2 and V1.11.1.

The following panel has changed:

```

zSecure Suite USER overview                               Line 1 of 39
Command ==>>>                                         Scroll==>>> CSR
All users                                               26 Nov 1998 07:47

_ Identification of ADGRANT                               IP01
  User name                                             AD GRANT_____
  Installation data                                     _____
  Owner                                                 SYSUSER_
  User's default group                                  SYSUSER_

  Group  Auth  R SOA AG Uacc  Revokedt  Resumedt  InstData
  _____
  SYSUSER_  USE  - - - - -  READ  _____
  SYS1     USE  - - - - -  READ  _____
  ADMGRP   JOIN - - - - -  Y    - - - - -  READ  _____

System access                                           Statistics
Revoked (may be by date)                               No_           Creation date           18Jul96
Inactive, revoked or pending                           No_           Last RACINIT current connects 20Jul00
Days of week user can logon                            SMTWTFS      User's last use date       20Jul00
Time of day user can logon                             _____   User's last use time       18:51
Date user will be revoked                               _____   (ddmmyyyy or NOREVOKE)
Date user will be resumed                               _____   (ddmmyyyy or NORESUME)

Password                                                 Password phrase
Has a password                                         Yes           Has a password phrase     Yes
Expired password                                       No_           Expired password phrase   No_
Password changed date                                 14Jan16      Password phrase change date 23May06
Password expiration date                              13Apr16      Password phrase expiry date 21Aug06
Old passwords present #                               1           Old pass phrases present #  2
Failed password attempts #                            0           Has a passw. phrase envelope No_
Password LEGACY encrypted                             No_           Pass phrase LEGACY encryped
Old passwords LEGACY enc. #                           0           Old pass phrase LEGACY enc. # 0
Password interval                                     90
Password interval in effect                            90
Mixed case password                                    Yes
Has a password envelope                               No_
Password disabled PROTECTED                           No_

Mandatory Access Control                               Privileges
Security label                                         _____   Security admin           SPECIAL No_
Security level                                         _____   DASD administrator OPERATIONS No_
Categories list                                         _____   Global audit set/list AUDITOR No_
Class authority                                         _____

Safeguards
Ignore UACC/Glob/* RESTRICTED                         No_
Log all user actions UAUDIT                            No_
Linked node.user Type Stat Pwd Defined (GMT) Approved (GMT) Creator
-----
Digital certificate labels                               Digital certificate names
-----

***** BOTTOM OF DATA *****

```

Figure 1. Detail Display

RACF Administration Guide: RA.U USER - User profile detail display

This update applies to zSecure Manager for RACF z/VM V1.11.1.

The password section in the following panel has changed:

```

zSecure Admin USER overview                               Line 1 of 45
Command ==>                                             Scroll==> CSR
like C##QA0*                                           5 Sep 2014 14:18

_ Identification of C##QA001                               DINO
User name                                               QA SUBJECT 001_____
Installation data                                       -----
Owner                                                  C##QA_
User's default group                                   C##QA_
                                                    Q.A. TESTSUBJECTS
                                                    Q.A. TESTSUBJECTS

Group  Auth  R SOA AG Uacc  Revokedt  Resumedt  InstData
C##QA_ CONNECT  - - - - NONE  - - - - - - - - Q.A. TESTSUBJECTS
C##CXCNG USE_  - - - - NONE  - - - - - - - - TEST GROUP DOR CNGR

System access                                           Statistics
Revoked (may be by date)                               No_      Creation date      18Jul12
Inactive, revoked or pending                           No_      Last RACINIT current connects 20Jul14
Days of week user can logon                            SMTWTFS  User's last use date  20Jul14
Time of day user can logon                             _____ User's last use time  18:51
Date user will be revoked                               _____ (ddmmyyyy or NOREVOKE)
Date user will be resumed                               _____ (ddmmyyyy or NORESUME)

Password                                                Password phrase
Has a password                                         Yes      Has a password phrase      Yes
Expired password                                       No_      Expired password phrase    No_
Password changed date                                  14Oct14  Password phrase change date _____
Password expiration date                               12Jan15  Password phrase expiry date _____
Old passwords present #                                __4      Old pass phrases present #  2__
Failed password attempts #                             __0      Has a passw. phrase envelope
Password LEGACY encrypted                              No_      Pass phrase LEGACY encrypted
Old passwords LEGACY enc. #                            __2      Old pass phrase LEGACY enc. # __2
Password interval                                       __90
Password interval in effect                             __90
Mixed case password                                     Yes
Has a password envelope
Password disabled PROTECTED No_

Mandatory Access Control                               Privileges
Security label                                         ----- Security admin          SPECIAL No
Security level                                         ----- DASD administrator OPERATIONS No
Categories list                                         ----- Global audit set/list AUDITOR No
Class authority                                         -----

Safeguards
Ignore UACC/Glob/* RESTRICTED No_
Log all user actions UAUDIT No_
Linked node.user Type Stat Pwd Defined (GMT) Approved (GMT) Creator
-----
Digital certificate labels    ___ Digital certificate names
-----

***** BOTTOM OF DATA *****

```

Figure 2. User profile detail display panel

The following rows were added to the table for **Password fields**:

Field	Description
Password LEGACY encrypted	This flag indicates if the current user password is hashed using a legacy algorithm. This field returns missing if the user does not have a password or if the user has the protected attribute.
Old passwords LEGACY enc. #	This field indicates how many passwords in the password history are hashed using a legacy algorithm. If SETROPTS PASSWORD(NOHIST) is in effect, RACF does not maintain a password phrase history. In that case, the PHRHIST_LEGACY_COUNT field is reported as missing.

The following rows were added to the table for **Password phrase fields**:

Field	Description
Has a passw. phrase envelope	This flag field indicates that the user profile contains a password phrase envelope with a decryptable form of the password phrase (that is, two-way encrypted).
Pass phrase LEGACY encrypted	This flag indicates if the current user password phrase is hashed using a legacy algorithm. This field returns missing if the user does not have a password phrase.
Old pass phrase LEGACY enc. #	This field indicates how many phrases in the password phrase history are hashed using a legacy algorithm. If SETROPTS PASSWORD(NOHIST) is in effect, RACF does not maintain a password phrase history. In that case, the PHRHIST_LEGACY_COUNT field is reported as missing.

RACF Administration Guide: RA.U USER - Additional selection-Attributes

This update applies to zSecure Manager for RACF z/VM versions V1.11.2 and V1.11.1.

The following panel has changed.

```

Menu  Options  Info  Commands  Setup
-----
zSecure Suite - RACF - User Attributes

Command ==>
Users like C##QAO*
Specify groups of criteria that the userids must meet:
Systemwide and group authorizations
OR_      _ Special      _ Operations      _ Auditor      _ Class auth
        _ Group-special  _ Group-oper      _ Group-audit

Logon status
OR_      _ Revoked      _ Inactive      _ Protected      _ Passw expired
        _ Revoked group  _ Certificate    _ Pass phrase    _ Phrase expired
        _ When day/time  _ ID mapping    _ Passw legacy   _ Phrase legacy

User properties
OR_      _ Has RACLINK  _ Restricted    _ User audited   _ Mixed case pwd

CKGRACF features
OR_      _ Queued cmds  _ Schedules    _ Userdata      _ MultiAuthority

Connect authority . >= 2_ 1. Use  2. Create  3. Connect  4. Join

```

Figure 3. User attribute selection

Three rows were added to the Advanced selection criteria for User attributes table:

Field	Description
ID Mapping	Selects based on whether an identity mapping is present.
Passw legacy	Selects based on whether the user has a password hashed using a legacy algorithm.
Phrase legacy	Selects based on whether the user has a password phrase hashed using a legacy algorithm.

RACF Audit Guide: SETROPTS - RACF settings report

This update applies to zSecure Manager for RACF z/VM versions V1.11.2 and V1.11.1.

The following panel changed:

```

RACF system, ICHSECOP, and general SETROPTS settings                               Line 1 of 67
Command ==> _____ Scroll==> PAGE
                                current settings
Complex System Collect timestamp
VR63 VR63 current settings

General RACF properties
Access Control active Yes
Force storage below 16M No
Check all connects GRPLIST Yes_____
Check genericowner for create No_____
NOADDCREATOR is active No_____
Dynamic CDT active No_____
Primary Language ENU
Secondary Language ENU
VMXEVENT control profile
RACF software release level
RACF DB template level

Data set protection options
Prevent duplicate datasets No
Protectall No_____
Automatic Dataset Protect Yes_____
Enhanced Generic Naming No_____
Prefix one-level dsns
Prevent uncataloged dsns No_____
GDG modelling No_____
USER modelling No_____
GROUP modelling No_____

DASD data set protection
Volume level permits DASDVOL No
Erase-on-scratch None
TAPE data set protection
Tape dataset check TAPEDSN No_____
Tape volume protection active No_____
Protection duration RETPD 00000____

Terminal protection
Terminal protection active No
Undefined terminal TERMUACC READ____
Program protection
Program control WHEN(PROGRAM) No_____
Program control mode Basic

Auditing options
Audit SPECIAL users Yes_____
Audit OPERATIONS users Yes_____
Audit USER profile changes Yes_____
Audit GROUP profile changes Yes_____
Audit SECLABELed resources No_____
Audit command violations Yes_____
Audit from security level None
Real datasetnames in SMF No_____
Dataset logoptions Profile
APPLAUDIT is active No_____
VMXEVENT audit profile

Mandatory Access Control options
Require SECLABEL MLACTIVE No_____
Prevent declassify MLS No_____
Stabilize labels MLSTABLE No_____
Label maintenance MLQUIET No_____
No SECLABEL tolerate COMPAT No_____
Special required SECL.CONTROL No_____
Req. labels UNIX fs MLFSOBJ _____
Req. labels IPC obj MLIPCOBJ _____
Name hiding active MLNAMES _____
Labels by system SECLBYSYSTEM _____

Identification/Authentication options
Remember dates INITSTATS Yes_____
Prevent logon if unused days _____180
Revoke after password attempt _____4
Old passwords forbidden 8
Password change wait days 1
Password change interval _____90
Password change warning day _____No
Mixed case passwords allowed No_____
Special passwd chars allowed YES_____
RACF password algorithm KDFAES_____
Key change required day 30_____

Job Entry Subsystem options
Batch userid req BATCHALLRACF No_____
Monitor userid req XBMALLRACF No_____
Call router exit EARLYVERIFY No_____
Default uid remote NJEUSERID ?????????
Default uid local UNDEFINEDU +++++++

RVARY passwords
RVARY SWITCH password set No
RVARY STATUS password set No

Password rules
Password rule 1
Password rule 2
Password rule 3
Password rule 4
Password rule 5
Password rule 6
Password rule 7
Password rule 8
Legend: $-national A-alpha c-mixed cons. C-consonant L-alphanum
m-mixed num N-numeric s-special v-mixed vowel V-vowel W-novowel
x-mixed all *-anything

***** Bottom of Data *****

```

Figure 4. RACF system, ICHSECOP, and general SETROPTS settings

RACF Audit Guide: SETROPTD - RACF SETROPTS settings in database

This update applies to zSecure Manager for RACF z/VM V1.11.1.

The following panel changed:

```

SETROPTS settings in database
Command ===> _____ Line 1 of 57
                          7 Dec 2015 14:05 Scroll====> PAGE

Complex
VR63

Dataset protection options
Protectall No_____
Automatic Dataset Protect Yes_____
Enhanced Generic Naming No_____
Prefix one-level dsns _____
Prevent uncataloged dsns No_____
GDG modelling No_____
USER modelling No_____
GROUP modelling No_____

General RACF properties
RACF Resource Access Ctl Fac HRF6030
Level of KERB processing _____
Check all connects GRPLIST Yes_____
Check genericowner for create No
NOADDCREATOR is active No_____
Application ID mapping stage _____
Primary Language ENU
Secondary Language ENU

DASD dataset protection
Volume level permits DASDVOL No
Erase-on-scratch None

Terminal protection
Terminal protection active No
Undefined terminal TERMUACC READ_____

TAPE dataset protection
Tape dataset check TAPEDSN No_____
Tape volume protection active No
Protection duration RETPD 00000_____

Program protection
Program control WHEN(PROGRAM) No_____

Auditing options
Audit SPECIAL users Yes_____
Audit OPERATIONS users Yes_____
Audit USER class changes Yes_____
Audit GROUP class changes Yes_____
Audit SECLABELed resources No_____
Audit command violations Yes_____
Audit from security level None
Real datasetnames in SMF No_____
Dataset logoptions Profile
APPLAUDIT is active No_____

Mandatory Access Control options
Require SECLABEL MLACTIVE No_____
Prevent declassify MLS No_____
Stabilize labels MLSTABLE No_____
Label maintenance MLQUIET No_____
No SECLABEL tolerate COMPAT No_____
Special required SECL.CONTROL No_____
Req. labels UNIX fs MLFSOBJ _____
Req. labels IPC obj MLIPCOBJ _____
Name hiding active MLNAMES _____
Labels by system SECLBYSYSTEM _____

Identification/Authentication options
Remember dates INITSTATS Yes_____
Prevent logon if unused days 180
Revoke after password attempt __4
Old passwords forbidden __8
Password change wait days __1
Password change interval _____90
Password change warning day _____No
Mixed case passwords allowed No_____
Special passwrld chars allowed YES_____
RACF password algorithm KDFAES_____
Key change required day __30_____

Job Entry Subsystem options
Batch userid req BATCHALLRACF No_____
Monitor userid req XBMALLRACF No_____
Call router exit EARLYVERIFY No_____
Default uid remote NJEUSERID ????????
Default uid local UNDEFINEDU ++++++

RVARY passwords
RVARY SWITCH password set No
RVARY STATUS password set No

Password rules
Password rule 1
Password rule 2
Password rule 3
Password rule 4
Password rule 5
Password rule 6
Password rule 7
Password rule 8
Legend: $-national A-alpha c-mixed cons. C-consonant L-alphanum
m-mixed num N-numeric s-special v-mixed vowel V-vowel W-novowel
x-mixed all *-anything
***** Bottom of Data *****

```

Figure 5. SETROPTS settings in database panel

Chapter 3. zSecure CARLa Command Reference

This chapter lists the updates for the *IBM Security zSecure CARLa Command Reference* as a result of the RACF password enhancement.

SELECT/LIST Fields: RACF

This update applies to zSecure Manager for RACF z/VM V1.11.1.

The following fields were added:

OLDPHRNX

This field contains the generation number of the entry in the history of the password phrase extension field. It is used to identify the history entries. This field forms a repeat group with field OLDPHRX. If RACF does not maintain a password history, the OLDPHRNX field is reported as missing.

OLDPHRX

This field contains the value of the entry in the history of the password phrase extension field. This field forms a repeat group with field OLDPHRNX. If RACF does not maintain a password history, the OLDPHRX field is reported as missing.

OPWDX

This field contains the value of the entry in the history of the password extension field. This field forms a repeat group with field OPWDXGEN. If RACF does not maintain a password history, the OPWDX field is reported as missing.

OPWDXCT

This field contains the number of entries in the history of the password extension field.

OPWDXGEN

This field contains the generation number of the entry in the history of the password extension field. It is used to identify the history entries. This field forms a repeat group with field OPWDX. If RACF does not maintain a password history, the OPWDXGEN field is reported as missing.

PHR_LEGACY

This flag indicates if the current user password phrase is hashed using a legacy algorithm. This field returns missing if the user does not have a password phrase.

PHRASEX

This field contains the password phrase extension for the user. If the user does not have a password phrase, or if the phrase is hashed using a legacy algorithm, the field is reported as missing.

PHRCNTX

This field contains the number of entries in the history of the password phrase extension field.

PHRHIST_LEGACY_COUNT

This field indicates how many phrases in the password phrase history are hashed using a legacy algorithm. If SETROPTS PASSWORD(NO HIST) is in effect, RACF does not maintain a password phrase history. In that case, the PHRHIST_LEGACY_COUNT field is reported as missing.

PWD_LEGACY

This flag indicates if the current user password is hashed using a legacy algorithm. This field returns missing if the user does not have a password or if the user has the protected attribute.

PWDHIST_LEGACY_COUNT

This field indicates how many passwords in the password history are hashed using a legacy algorithm. If SETROPTS PASSWORD(NO HIST) is in effect, RACF does not maintain a password history. In that case, the PWDHIST_LEGACY_COUNT field is reported as missing.

PWDX

This field contains the password extension of the user. If the user does not have a password, or if the password is hashed using a legacy algorithm, the field is reported as missing.

SELECT/LIST Fields: SETROPTS

This update applies to zSecure Manager for RACF z/VM V1.11.1.

The following rows were added to the table for PWDRULE1:

Pattern character	Meaning
s	Special
x	Mixed all

The following fields were added:

RACF_PWD_ALGORITHM

This field shows the password algorithm in effect. [Table 2 on page 10](#) lists the possible values for this field. The value is missing if the template level of the RACF database is too low to support this setting.

<i>Table 2. Possible values for RACF_PWD_ALGORITHM</i>	
Value	Meaning
KDFAES	The KDFAES algorithm is used. This is a more secure encryption of the password and password phrase.
LEGACY	Is DES or the algorithm as is indicated by the ICHDEX01 password encryption exit (masking, DES, or installation-defined encryption method).

RACF_PWD_SPECIAL_CHAR

This flag field indicates whether special characters are allowed in passwords. The value is missing if the template level of the RACF database is too low to support this setting. For details about allowed special characters, see the documentation in the *RACF Security Administrator's Guide*.

SELECT/LIST Fields: SYSTEM

This update applies to zSecure Manager for RACF z/VM V1.11.1.

The following rows were added to the table for PWDRULE1:

Pattern character	Meaning
s	Special
x	Mixed all

The following fields were added:

RACF_PWD_ALGORITHM

This field shows the password algorithm in effect. [Table 3 on page 10](#) lists the possible values for this field. The value is missing if the system's software level is too low to support this setting.

<i>Table 3. Possible values for RACF_PWD_ALGORITHM</i>	
Value	Meaning
KDFAES	The KDFAES algorithm is used. This is a more secure encryption of the password and password phrase.
LEGACY	Is DES or the algorithm as is indicated by the ICHDEX01 password encryption exit (masking, DES, or installation-defined encryption method).

RACF_PWD_SPECIAL_CHAR

This flag field indicates whether special characters are allowed in passwords. The value is missing if the system's software level is too low to support this setting. For details about allowed special characters, see the documentation in the *RACF Security Administrator's Guide*.

Chapter 4. zSecure Messages Guide

This chapter lists the updates for the *IBM Security zSecure Messages Guide* as a result of the RACF password enhancement. These updates apply to zSecure Manager for RACF z/VM V1.11.1.

CKR2231 **Password support for special characters not enabled on current system**

Explanation

The source database in a merge operation allows special characters in passwords, but the current database does not. If passwords are copied from the source database to the current database, users with a password containing special characters will not be able to login using this password.

Severity

0

CKR2232 **Current system does not support KDFAES encryption**

Explanation

The source database in a merge operation uses the KDFAES encryption algorithm for password hashing, but the current database does not. Commands will not be generated to copy passwords from the source database to the current database.

Severity

0

CKR2521 **Profile should not have been translated**

Explanation

This internal error message indicates an inconsistency in the MERGE internal record structure.

User response:

See the [Electronic Support Web site](#) for possible maintenance associated with this message. If you cannot find applicable maintenance, follow the procedures described in [../DITA_shared_files/contactingsoftwaresupport.dita](#) to report the problem.

Severity

24

CKR2522 **Profile should not have been src-only**

Explanation

This internal error message indicates an inconsistency in the MERGE internal record structure.

User response:

See the [Electronic Support Web site](#) for possible maintenance associated with this message. If you cannot find applicable maintenance, follow the procedures described in [../DITA_shared_files/contactingsoftwaresupport.dita](#) to report the problem.

Severity

24

