IBM Security zSecure RACF Password Service Stream Enhancement

Documentation updates

IBM Security zSecure RACF Password Service Stream Enhancement

Documentation updates

Contents

Chapter 1. About this document

Several enhancements were made to RACF to improve the security of passwords and password phrases. The IBM® Security 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
- Define users with a password phrase and no password
- 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 Audit SMF reporting function: RACF commands can have extra keywords and parameters.

These updates apply to IBM Security zSecure versions V2.1.1 and V2.1.0 and some of them also apply to V1.*x.x*. The zSecure Admin updates only apply to versions V2.1.1 and V2.1.0. For other versions, support is limited to issuing warning and error messages when a user action might otherwise result in an incorrect change to a RACF user profile.

This document lists the updates for these enhancements to the IBM Security zSecure V2.1.1 documentation:

IBM Security zSecure Release Information

IBM Security zSecure Admin and Audit for RACF User Reference Manual, LC27-5639-01

IBM Security zSecure CARLa Command Reference, LC27-6533-00

IBM Security zSecure Command Verifier User Guide, SC27-5648-01

IBM Security zSecure Visual Client Manual, SC27-5647-01

IBM Security zSecure Messages Guide, SC27-5643-01

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.
- Changes resulting from support of the RACF password enhancements for IBM Security zSecure CICS® Toolkit did not result in any documentation changes.

Chapter 2. zSecure Release Information

This chapter lists the updates for the IBM Security zSecure *Release Information* as a result of the RACF password enhancement for V2.1.1.

Support for the RACF password enhancements in IBM Security zSecure Admin and Audit versions V1.12, V1.13.0, and V1.13.1 is limited to issuing warning and error messages when a user action might otherwise result in an incorrect change to a RACF user profile.

Incompatibility warnings

The following items were added:

Authorization of CKGRACF USER subcommand options

The resource names as they are actually used for the authorization verification have been changed. They now reflect the resource names as they are already documented in the CKGRACF chapter of the *User Reference Manual*. The resource names that are affected are:

Table 1. Resource names and required access

USER subcommand	Resource name checked	Access required
PWSET NOPASSWORD	CKG.CMD.USER.*action*.PWSET.NOPASSWORD Previously used value: CKG.CMD.USER.*action*.PWSET.NOPASSWD	UPDATE
PWSET RANDOM	CKG.CMD.USER.*action*.PWSET.RANDOM Previously used value: CKG.CMD.USER.*action*.PWSET.NOPASSWD	UPDATE

The documented value for the resource name checked when using the NONEXPIRED option has been corrected to reflect the actual resource name checked.

Table 2. Resource names and required access

USER subcommand	Resource name checked	Access required
PWSET NONEXPIRED	CKG.CMD.USER.*action*.PWSET.NONEXP Previously documented value: CKG.CMD.USER.*action*.PWSET.NONEXPIRED	UPDATE

If you have defined profiles that match the previously used or documented values, you must change these profiles to match the new resource names.

Coexistence considerations

If you use one of the new CKGRACF functions, older versions of CKGRACF might issue error messages CKG651I and CKG639I. This especially applies if you create queued commands that require actions by a second or third administrator. Only generate queued commands that exploit new functions when all systems that share the RACF database have been upgraded to the same level, or make sure that CKGRACF commands are only issued from a system with the higher level of the CKGRACF code.

Chapter 3. zSecure Admin and Audit for RACF User Reference Manual

This chapter lists the updates for the *IBM Security zSecure Admin and Audit for RACF User Reference Manual* as a result of the RACF password enhancement.

Introduction: A sample run

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

The following panel has changed:

```
zSecure Suite USER overview                                    Line 1 of 49
Command ===>                                                   Scroll===> CSR
All users                                      26 Nov 2014 07:47


_ Identification of ADGRANT                                            IPO1
  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                 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     ___________  (ddmmmyyyy or NOREVOKE)
  Date user will be resumed     ___________  (ddmmmyyyy 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
  ____________________________
  Certificate filter label

  ____________________________
  Identity mapping label   Identity mapping filter                      Identi
_ myFirstRACMAP            UID=armeBert,OU=Tools Development,O=IBM,C=NL  ldaps.c
```

Figure 1. Detail Display

RACF Administration Guide: Line commands on profile displays

The ML and P line commands have changed. This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

ML - Manage logon information

Use the **ML** line command for the following tasks:

- Revoke or resume a user either now or at a future date using a RACF® function. To work with CKGRACF revoke/resume schedules, use the **MS** (CKGRACF Schedule) line command instead of this one.
- Change the password interval for a user ID.
- Set or delete the CKGRACF default password or phrase for a user ID.

This command is only supported if zSecure Admin is installed and active.

When you issue the **ML** line command, the panel shown in Figure 2 opens.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Manage logon-data
Command ===>

Userid . . . . . : ADM1

Revoke date  . . . . ____________ (dd mmm yyyy, ddmmmyyyy, yyyy-mm-dd, or NOW)
Resume date  . . . . ____________ (dd mmm yyyy, ddmmmyyyy, yyyy-mm-dd, or NOW)

Password interval    30_  (NO or number)


Specify default value
Select password or phrase        Select action
_  1. Password                   _  1. Set value
   2. Phrase                        2. Remove value

New password value
==>           ==>
```

Figure 2. LOGON DATA panel

The user you are working with is shown at the top.

To revoke or resume the user immediately, type *NOW* in the revoke date or resume date field. To perform the action at a later date, enter the date instead in one of the following date formats:

- *ddmmmyyyy*, 01jan2002 for example.
- *dd mmm yyyy*, 01 jan 2002 for example.
- *yyyy-mm-dd*, 2002-01-01 for example.

To set up a password that does not require the user to change it, specify *NO* for the password interval. To specify a password interval, enter the number of days up to a maximum of 254.

To set a CKGRACF default password, select **1 password** and action **1 Set value**. Then, enter the password twice. To set a CKGRACF default password phrase, select **2 Phrase** and action **1 Set value**.

To delete a CKGRACF default password or phrase, select **2 Delete**. Do not select a default password or phrase action if you want it to be empty. To retain the CKGRACF default password or phrase, do not select a default password action.

If you set a CKGRACF default password or phrase for a user, it does not change the current password or phrase. To change the current password or phrase to this value, run the **P** (Password) line command.

P - Change password or phrase and resume user

Use the **P** (Password) line command for managing password and password phrases and resuming user IDs. When you issue this command, the User PASSWORD/PHRASE panel opens. This command is only supported if

zSecure Admin is installed and active.

```
 Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                      zSecure Suite - RACF - User password/phrase
 Command ===> ____________________________________________________________

 Userid  . . . . . . . : USR0001
 Name  . . . . . . . . : USER 0001
 Instdata  . . . . . . : TESTUSER FOR 2000-TEST, ESPECIALLY TO TEST THE    RACF DAT
 Last use date . . . . : 09Sep2014  Last use time . . . : 03:45
 Password changed  . . : 04Aug2014  Phrase changed  . . :
 Revoked . . . . . . . : No         Revoke inactive . . : No
 Revoke date . . . . . :            Resume date . . . . :
 Has a password  . . . : Yes        Has a phrase  . . . : No
 Protected . . . . . . : No

 Select password or phrase:  Select action:            Options:
 2  1. Password              3  1. No change           /  Expired
    2. Phrase                   2. Remove             /  Resume userid
    3. Protected                3. Specify new value  /  Ignore history
    4. NoProtected              4. Set to default        Bypass exits
                                5. Set to previous       Bypass rules
 New password value             6. Set to random
 ==>           ==>
```

Figure 3. User PASSWORD/PHRASE panel

The RACF User PASSWORD/PHRASE panel has the following fields of interests:

Userid
Displays the selected user ID and the following related information:

- User name.
- Installation data.
- Last date and time the user ID was used.
- Date of the last password and password phrase change.
- A flag indicating whether the user ID has been revoked.
- If the user ID has been revoked and resumed, the revoke and resume dates are listed.
- A flag indicating whether the user ID is protected.
- Flags indicating whether the user has a password or phrase
- Current setting for the *Revoke inactive attribute* that indicates whether the user is effectively revoked due to the `SETROPTS INACTIVE()` setting.

Password/phrase actions
You can select **Password** or **Phrase** and select one of the following actions:

No change
For CKGRACF, a `PWSET CURRENT` command is generated. For RACF, this action only applies when you select Resume.

Remove
Removes the password or password phrase.

Specify new value
This action allows you to set a new password or password phrase. You must specify the new password twice on this panel. For password phrase, a follow-on panel is displayed.

Set to default
Applies to CKGRACF only. This action allows you to reset the password or phrase to the default value.

Set to previous
Applies to CKGRACF only. This action allows you to reset the password or phrase to the previous value.

Set to random
Applies to CKGRACF only. This action allows you to set a random password or phrase.

With option **Protected** you can assign the protected attribute to the userid. Option **NonProtected** applies to CKGRACF only and removes the protected attribute. To remove the protected attribute with a RACF command, set a password or phrase for the userid.

Options
You can select each of the following options by placing a forward slash (/) in front of them:

Expired
Specifies that the user must change the password or phrase at the next login.

Resume userid
Specifies the user ID to be resumed. This option can be specified without resetting the password or phrase.

Ignore history
Use this option to disable the history check that CKGRACF performs when a password or phrase is set.

Ignore rules
Use this option to disable the password or phrase rule check that CKGRACF performs when a password or phrase is set.

Bypass exits
Use this option to disable the ICHPWX01 or ICHPWX11 exit call from CKGRACF when a password or phrase is set.

Note:

1. Setting a non-expired password or phrase might require more authorization than setting an expired one.
2. You can set the CKGRACF default password or phrase through the **ML** Manage Logon information line command.

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

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

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___                      Q.A. TESTSUBJECTS
_ User's default group         C##QA___                      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     __________ (ddmmmyyyy or NOREVOKE)
  Date user will be resumed     __________ (ddmmmyyyy 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
_ DINO.C##QAWT     Peer    Sync ___  2013/09/10 11:09 2013/09/10 11:26 C##QA001
  Digital certificate labels       Digital certificate names
  Primary____________________      6F.Jones@Zsecur.NL.CN=Root.OU=CryptoLab.O=Co
  Certificate filter label
  _____________________________
  Identity mapping label           Identity mapping filter
_ myFirstRACMAP                    UID=armeBert,OU=Tools Development

  UsrNm   Flg UsrData
_ PHONE    00 +31-15-2513333
  CKGRACF authority requirement
_ Authority setting DUAL set by C##BGUI at 18 Nov 1997 16:00
  Scheduled events
_ Scheduled event: Schedule 'QA#UIT' disable  2 Sep 2001; set by C##QA1G at  2
_ Queued command (R): USER C##QA001 SCHEDULE HELPDESK ENABLE (01Mar2015:02Mar20
  Inactive commands
_ Queued command (E): USER C##QA001 SCHEDULE HELPDESK DISABLE (30Aug2014:31Aug2
  Commands that have been executed
_ Queued command (CA): USER C##QA001 SCHEDULE QA#UIT DISABLE (02Sep2014); reque
  Other CKGRACF data
_ Default password set by C##BLU1 at  5 Nov 2013 09:37
****************************** BOTTOM OF DATA ********************************
```

Figure 4. 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 history. In that case, the PWDHIST_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 history. In that case, the PWDHIST_LEGACY_COUNT field is reported as missing.

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

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

The following panel has changed.

```
  Menu   Options   Info   Commands   Setup
------------------------------------------------------------------------------
                        zSecure Suite - RACF - User Attributes
Command ===>
Users like C##QA0*
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 5. User attribute selection

Two rows were added to Table 3 on page 12:

Table 3. Advanced selection criteria for User attributes

Field	Description
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 passphrase hashed using a legacy algorithm.

RA.H HELPDESK - One-panel help desk options

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

The menu option **RA.H** (HELPDESK) can be used to perform the most common user administration tasks, and is especially designed for use by a decentralized or centralized help desk. If your installer chose to follow the suggestions in the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*, it can also be started directly from ISPF by typing CKGHELP. The menu is displayed in Figure 6.

```
  Menu       Options       Info       Commands       Setup        Startpanel
--------------------------------------------------------------------------------
                          zSecure Suite - RACF - Helpdesk
Option  ===> ____________________________________________________________

1    List            List RACF profile information
2    Password/Phrase Set a new password or phrase
3    Default         Set the password or phrase to the user's default value
4    Previous        Set the password or phrase to the previous value
5    Resume          Resume a userid after too many invalid attempts
6    Disable         Temporarily disable logon for a userid
7    Enable          Allow user to logon after a Disable
8    Set default     Define a default password or phrase for a userid

Userid . . . . . ________   (type userid and press enter)
Password or phrase . . . . _  1. Password  2. Phrase
New password . . . . . .           Verify password  .
Reason . . . . . ____________________________________________________
Workflow option  . . . . . 1  1. Request   2. Withdraw  3. Approve  4. Deny
```

Figure 6. HELPDESK Menu

For a decentralized help desk, options 6 to 8 would typically be omitted from the panel by setting the access level to *NONE* on SAF resources CKR.OPTION.RA.H options 6 through 8. The setup of the help panel contents can be done using XFACILIT CKR.OPTION.RA.H profiles on a by-user or by-group basis.

Most of the options shown on this panel are familiar to a RACF administrator; the exception is the *default password or phrase*. The default password or phrase is an installation-defined option added by zSecure. This is an additional and inactive password or phrase that can only be set by selected administrators. The user must know the value of this default password or phrase. A larger group of administrators, like help desk personnel, can *apply* the default password or phrase. In this way, the administrators can reset the user password or phrase to a predetermined value, even if both the original and new passwords or phrases are not known to them.

Enter the **Userid** you want to act on, select an option, and enter any additional fields required for that option, then press **Enter**.

The following options can be specified on the Help desk panel:

List List RACF information about this user. For more information, see LIST for details.

Password/Phrase
Set a new password or phrase for the user. Type the new password twice in the appropriate fields. For a password phrase, a follow-on panel is displayed. The user must always change the password or phrase at the next logon.

Default
Set the user password or phrase to the default value. If none has been defined yet, you are prompted for one.

Previous
Set the user password or phrase to the previous value.

Resume
Resume the user. This operation only succeeds if all `CKGRACF` schedules indicate that the user can have access to the system.

Disable
Change the user schedule so that the user cannot logon. This change can be accomplished by a hard revoke or soft revoke depending on the user authority. If the user has READ access to SYSADMIN, then that schedule name is used for a hard revoke. If the user has access to GRPADMIN but not SYSADMIN, then the GRPADMIN schedule name is used for a soft revoke. Otherwise, a default schedule accessible to the user is employed.

Enable
Change the schedule of the user so that he can logon as far as the help desk user is concerned. Note however that both schedule names GRPADMIN and SYSADMIN must agree before the user can actually work. That is, neither soft-revokes or hard-revokes have been requested.

Set Default
This sets the default password or phrase of a user for use by a help desk. This option should therefore not be available to that help desk.

The normal **Request type** for an administrator to use is `REQUEST`. If you are unauthorized to `REQUEST` the action, your installation might permit you to `ASK` for it. That is, add the action to the administrator queue for approval. If you specify `WITHDRAW`, you are attempting to undo a previous `ASK` or `REQUEST`. If an action has not been performed, you can `DENY` it to cancel the operation.

RACF Administration Guide: Reviewing queued commands

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

When you use the `I` line command on the Queued Command detail panel and then select the **Request a password or password phrase** action, the system displays the Request a command panel - password and phrase commands. This panel has changed, as well as the field descriptions.

```
 Menu  Options  Info  Commands  Setup
------------------------------------------------------------------------------
                        zSecure Suite - Request a command
Command ===> ____________________________________________________________

Userid  . . . . . . . CRMBMR2

Select password or phrase:  Select action:            Options:
5  1. Password              6  1. No change           /  Expired
   2. Phrase                   2. Remove                 Resume userid
   3. Protected                3. Specify new value      Ignore history
   4. NoProtected              4. Set to default         Bypass exits
   5. Interval                 5. Set to previous        Bypass rules
                               6. Set to random

New password  . . . .          (type new password)
Verify password . . .          (type new password again)
Interval                       (0-254, or NO for no interval)
Request type  . . . .          A(sk), R(equest) or W(ithdraw)
```

Figure 7. Request a command panel - password and phrase commands

The Request a password/phrase panel has the following fields of interests:

Password/phrase actions
You can select **Password** or **Phrase** and select one of the following actions:

No change
A PWSET CURRENT command is generated.

Remove
Removes the password or password phrase.

Specify new value
This action allows you to set a new password or password phrase. You must specify the new password twice on this panel. For password phrase, a follow-on panel is displayed.

Set to default
This action allows you to reset the password or phrase to the default value.

Set to previous
This action allows you to reset the password or phrase to the previous value.

Set to random
This action allows you to set a random password or phrase.

Protected
This action allows you to assign the protected attribute to the userid.

NonProtected
This action allows you to remove the protected attribute.

Interval
This option allows you to set the password interval. Enter 0-254 for a specific password interval or N for no interval. When no value is entered, the SETROPTS password interval setting is used.

Options
You can select each of the following options by placing a forward slash (/) in front of them:

Expired
Specifies that the user must change the password or phrase at the next login.

Resume userid
Specifies the user ID to be resumed. This option can be specified without resetting the password or phrase.

Ignore history
Use this option to disable the history check that CKGRACF performs when a password or phrase is set.

Ignore rules
Use this option to disable the password or phrase rule check that CKGRACF performs when a password or phrase is set.

Bypass exits
Use this option to disable the ICHPWX01 or ICHPWX11 exit call from CKGRACF when a password or phrase is set.

Request type
A CKGRACF parameter for multiple-authority, normally set to REQUEST. In some installations, end users might be permitted to ASK for permissions. A request that is not authorized to be run immediately shows up in the administrator approval queue for review. To retract a request in the approval queue (either due to ASK or because of a DUAL or TRIPLE authority requirement) specify WITHDRAW.

RACF Audit Guide: SETROPTS - RACF settings report

This update applies to zSecure Audit versions V2.1.0 and V2.1.1.

The following panel changed:

```
RACF system, ICHSECOP, and general SETROPTS settings              Line 1 of 67
Command ===> ____________________________________________________ Scroll===> CSR_

   Complex  System   Collect time stamp
   DINO     DINO     23 Mar 2014 00:07

General RACF properties                Data set protection options
Access Control active          Yes     Prevent duplicate datasets    No
Force storage below 16M        No      Protectall                    Yes/fail
Check all connects  GRPLIST    Yes_____ Automatic Dataset Protect    No______
Check genericowner for create  Yes_____ Enhanced Generic Naming      Yes_____
NOADDCREATOR is active         Yes_____ Prefix one-level dsns        ONEQUAL_
Dynamic CDT active             No      Prevent uncataloged dsns      No______
RACF local node                DINO    GDG modelling                 No______
RRSF propagate RACF commands   No      USER modelling                No______
RRSF propagate applications    No      GROUP modelling               No______
RRSF propagate passwords       No
RRSF honour RACLINK PWSYNC     Yes
Application ID mapping stage   0
Level of KERB processing       __0
Primary Language               ENU
Secondary Language             ENU
RACF software release level    HRF7707 OA03853
RACF DB template level         OA03853

DASD data set protection               Terminal protection
Volume level permits DASDVOL   No      Terminal protection active    Yes
Erase-on-scratch               All     Undefined terminal TERMUACC   NONE____

TAPE data set protection               Program protection
Tape dataset check TAPEDSN     No______ Program control WHEN(PROGRAM) Yes_____
Tape volume protection active  Yes     Program control mode          Basic
Protection duration RETPD      00000___

Auditing options                       Mandatory Access Control options
Audit SPECIAL users            Yes_____ Require SECLABEL     MLACTIVE No______
Audit OPERATIONS users         Yes_____ Prevent declassify   MLS      No______
Audit USER profile changes     Yes_____ Stabilize labels     MLSTABLE No______
Audit GROUP profile changes    Yes_____ Label maintenance    MLQUIET  No______
Audit SECLABELed resources     No______ No SECLABEL tolerate COMPAT   No______
Audit command violations       Yes_____ Special required SECL.CONTROL No______
Audit from security level      None    Req. labels UNIX fs  MLFSOBJ
Real datasetnames in SMF       No______ Req. labels IPC obj  MLIPCOBJ
Dataset logoptions             Profile  Name hiding active   MLNAMES
APPLAUDIT is active            No______ Labels by system SECLBYSYSTEM

Identification/Authentication options  Job Entry Subsystem options
Remember dates INITSTATS       Yes_____ Batch userid req BATCHALLRACF Yes_____
Prevent logon if unused days   255_____ Monitor userid req XBMALLRACF No _____
Revoke after password attempt  __5_____ Call router exit  EARLYVERIFY No _____
Old passwords forbidden        _32      Default uid remote  NJEUSERID ????????
Password change wait days      _No      Default uid local  UNDEFINEDU ++++++++
Password change interval       _90_____ JOBCLASS/SUBMITTER access ctl No
Password change warning day    _10_____ JOBCLASS/OWNER access ctl     Yes
Mixed case passwords allowed   No______
Special passwrd chars allowed  No______ RVARY passswords
RACF password algorithm        LEGACY__ RVARY SWITCH password set    No
Key change required day        ___30___ RVARY STATUS password set    No

Password rules
Password rule 1
Password rule 2                LLLLL*** LENGTH(5:8)
Password rule 3
Password rule 4
Password rule 5                L*C*CN** LENGTH(6:8)
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

Generic Anchor settings
Generic anchors system count     5
Jobname  Count
TESTJOB*     6

EIM registry
NONE
```

Figure 8. RACF system, ICHSECOP, and general SETROPTS settings

RACF Audit Guide: SETROPTD - RACF SETROPTS settings in database

This update applies to zSecure Audit versions V2.1.0 and V2.1.1.

The following panel changed:

```
SETROPTS settings in database                                  Line 1 of 55
Command ===> _____________________________________________ Scroll===> CSR_
                                          22 Aug 2014 00:07
   Complex
   DINO

Dataset protection options            General RACF properties
Protectall                  Yes/fail  RACF Resource Access Ctl Fac  2.6.0
Automatic Dataset Protect   No_____   Level of KERB processing
Enhanced Generic Naming     Yes____   Check all connects  GRPLIST   Yes____
Prefix one-level dsns       ONEQUAL_  Check genericowner for create Yes____
Prevent uncataloged dsns    No_____   NOADDCREATOR is active        Yes____
GDG modelling               No_____   Application ID mapping stage
USER modelling              No_____   Primary Language              ENU
GROUP modelling             No_____   Secondary Language            ENU

DASD dataset protection               Terminal protection
Volume level permits DASDVOL  No      Terminal protection active    No
Erase-on-scratch              All     Undefined terminal TERMUACC   READ___

TAPE dataset protection               Program protection
Tape dataset check TAPEDSN    No_____ Program control WHEN(PROGRAM) Yes____
Tape volume protection active Yes
Protection duration RETPD     00000___

Auditing options                      Mandatory Access Control options
Audit SPECIAL users           Yes____ Require SECLABEL     MLACTIVE No_____
Audit OPERATIONS users        Yes____ Prevent declassify   MLS      No_____
Audit USER profile changes    Yes____ Stabilize labels     MLSTABLE No_____
Audit GROUP profile changes   Yes____ Label maintenance    MLQUIET  No_____
Audit SECLABELed resources    No_____ No SECLABEL tolerate COMPAT   No_____
Audit command violations      Yes____ Special required SECL.CONTROL No_____
Audit from security level     None    Req. labels UNIX fs  MLFSOBJ
Real datasetnames in SMF      No_____ Req. labels IPC obj  MLIPCOBJ
Dataset logoptions            Profile_ Name hiding active  MLNAMES
APPLAUDIT is active           No_____ Labels by system SECLBYSYSTEM

Identification/Authentication options  Job Entry Subsystem options
Remember dates INITSTATS      Yes____ Batch userid req BATCHALLRACF Yes____
Prevent logon if unused days  255____ Monitor userid req XBMALLRACF No_____
Revoke after password attempt __5____ Call router exit  EARLYVERIFY No_____
Old passwords forbidden       _32     Default uid remote  NJEUSERID ????????
Password change wait days     _No     Default uid local  UNDEFINEDU ++++++++
Password change interval      _90____
Password change warning day   _10____
Mixed case passwords allowed  No_____
Special passwrd chars allowed No_____ RVARY passswords
RACF password algorithm       LEGACY__ RVARY SWITCH password set    No
Key change required day       ___30___ RVARY STATUS password set    No

Password rules
Password rule 1
Password rule 2               LLLLL*** LENGTH(5:8)
Password rule 3
Password rule 4
Password rule 5               L*C*CN** LENGTH(6:8)
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 9. SETROPTS settings in database panel

RACF-Offline: The Offline RACF environment

This update applies to zSecure Admin versions V1.12, V1.13.0, V1.13.1, V2.1.0, and V2.1.1.

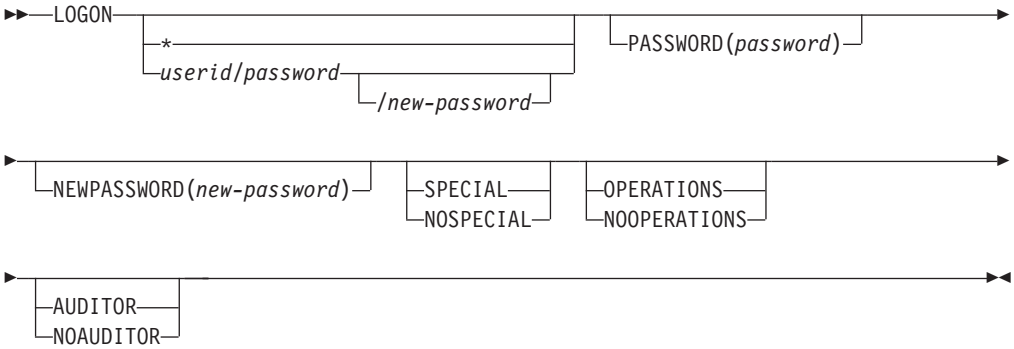
The third item in the bulleted list changed:

- Commands are parsed according to the settings of the active system. This includes various SETROPTS settings (GENERIC, GENCMD, EGN, and SPECIALCHARS) and the dynamic parsing (as set by the IRRDPI00 command). A fully initialized version of RACF on the active system is required.

RACF-Offline: LOGON command

The syntax and description of the LOGON command changed. This update applies to zSecure Admin versions V1.12, V1.13.0, V1.13.1, V2.1.0, and V2.1.1.

The LOGON command results in using the RACF definitions, authorizations, and attributes of an ID from the Offline RACF database. Failure to use the LOGON command might result in various types of errors. This command is applicable only in the B8RACF environment. The LOGON command has the following syntax:



Use the LOGON command to retrieve the definition and attributes of your ID from the Offline RACF database. If you do not use the LOGON command, the definition and attributes of your ID in the system RACF database are used for commands issued against the Offline database. This might result in various types of errors.

If you enter just the LOGON command without any parameters, the current ID is used to LOGON to the Offline RACF database. If you specify a *userid*, you must also specify the *password* of that ID. You can specify the password following a forward slash (/) after the *userid*. The preferred method is to use the PASSWORD keyword to specify the current password of the ID.

If you want to be prompted for the password in non-display mode, end the *userid* with a forward slash (/), or specify the PASSWORD keyword without any parameters. For example:

```
You:    LOGON ibmuser PASSWORD
System: IKJ56700A ENTER Current password -
You:     <non-displayed-password>
```

If you specify the current password, you can also specify a new password. To be prompted for the new password in non-display mode, end the current password with a forward slash (/), or specify the NEWPASSWORD keyword.

If your current password or new password contains special characters, specify it using the PASSWORD or NEWPASSWORD keywords. Alternatively, you can specify the password within single quotation marks.

You can also explicitly specify that you want to logon using your current *userid* by using an asterisk (*). You do not need to specify a password, but if you do specify a password through the PASSWORD keyword, it is verified during subsequent processing.

The optional attribute keywords (NO)SPECIAL, (NO)OPERATIONS, and (NO)AUDITOR request that the effective value of the specified attribute is temporarily set or reset after logging on to the Offline RACF database. The value of the attribute in the Offline RACF database itself is not changed. Use of these keywords requires access to the B8R.*attribute.master-racfdb-name* resource in the XFACILITY resource class in the System RACF database. For more information about the required authorization see "Command authorization verification" in the *IBM Security zSecure Admin and Audit for RACF User Reference Manual*.

If you specify one of the optional attribute keywords, you also must specify a value for the *userid*, including the *password*, or use an asterisk to logon using your current ID. When using an optional attribute keyword, password prompting using the forward slash (/) is not supported.

CKGRACF command reference: FIELD command

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

New fields `PHRASEX` and `PWDX` were added to the tables Table 4 and Table 5. The last note was also changed.

Table 4. Fields for CKGRACF FIELD

Name	Meaning	Length	Format
PHRASEX	Password phrase extension	Variable, up to 40 characters	'xxxx...xx'x
PWDX	Password extension	Variable, up to 40 characters	'xxxx...xx'x

Table 5. Command access checks for CKGRACF FIELD

Field	Resource name checked	Access required
`PHRASEX`	`CKG.CMD.FIELD.PHRASEX` (See Note about password-related fields.)	READ for the LIST option, UPDATE for all other options.
`PWDX`	`CKG.CMD.FIELD.PWDX` (See Note about password-related fields.)	READ for the LIST option, UPDATE for all other options.

Note:

The `FIELD` command is not subject to scope checks. Because the `PASSWORD`, `PHRASE`, `PHRASEX`, and `PWDX` fields can be used to list all users' encrypted password information, make sure that access to the field is restricted. Access to these fields should be only be granted to users who are also allowed to read the active RACF database in unrestricted mode.

CKGRACF command reference: SHOW command

This update applies to zSecure Admin versions V2.1.0 and V2.1.1.

The following command profile-related resources that are reported by `CKGRACF SHOW MYACCESS [id]` were changed or added to the list:

CKG.CMD.USER.REQ.PHRESET
CKG.CMD.USER.REQ.PWSET.NOPASSWORD
CKG.CMD.USER.REQ.PWSET.NOPHRASE
CKG.CMD.USER.REQ.PWSET.NOPROTECTED
CKG.CMD.USER.REQ.PWSET.PASSWORD
CKG.CMD.USER.REQ.PWSET.PHRASE
CKG.CMD.USER.REQ.PWSET.PROTECTED

CKGRACF command reference: USER command

Various changes were made to the USER command. These updates apply to zSecure Admin versions V2.1.0 and V2.1.1. The changed sections are included.

Note: Referenced topics that have not changed are not included in this document. You can find them in the *IBM Security zSecure Admin and Audit for RACF User Reference Manual*.

USER

The USER command can be used for centralized and decentralized user maintenance. Functions provided are, for example, setting of passwords and password phrases, and management of access to the system using revoke/resume schedules. Authority to issue the command is controlled using RACF profiles. The command is also subject to the multiple-authority settings. Managing revoke/resume schedules is controlled using authority to the named schedule. Both multiple-authority settings and schedules are explained in this section.

The USER command has the following syntax:

```
USER userid subcommand ...  [ action ] [ REASON(reason) ]

 userid     Any valid RACF userid.
 subcommand A USER subcommand; see "Specifying USER subcommands"; one or more
            different subcommands can be specified.
 action     A queued-command action; see "Specifying Queued-command actions" on page 22;
            the default, REQUEST, performs the command for a single-authority
            userid.
 reason     A reason string (See Reason keywords in CKGRACF).
```

Specifying USER subcommands

A single `USER` command can include multiple subcommands. Some subcommands are mutually exclusive. If an error occurs in any of the subcommands when the `USER` command is processed, the target profile is not changed.

The following *subcommands* can be specified.

- `INTERVAL(value)`
- `NOINTERVAL`
- `PHRESET`
- `PWDEFAULT [password or phrase options]`
- `PWNOEXIT`

- PWNOHIST
- PWNORULE
- PWRESET
- PWSET [*password or phrase options*] [*expired-option*]
- RACLINK UNDEF[(*node.id*)]
- RESUME
- SCHEDULE*scheduleaction* [*date*] [*reason*]

See "USER subcommands" on page 23 for more information about each subcommand.

Specifying Queued-command actions

The USER command supports all queued-command actions. You can also use abbreviations of the queued-command actions. The following actions can be specified:

- ASK for ASK
- REQ for REQUEST
- WITHDRAW
- SEC for SECOND
- CMP for COMPLETE.

If no queued-command action is specified, REQUEST is used. If SECOND or COMPLETE is specified without further qualification, APPROVE is used.

When a queued command is re-entered for a stage following REQUEST, the following processing occurs:

- The PROMPT option does not prompt again.
- The value specified for the PASSWORD or PHRASE is ignored.
- The REASON keyword is ignored.

See Actions on queued commands for information about these actions.

Access checking

The type of access checking done for a USER command depends on the options specified on the command. See the following topics for more information.

- "Access checks for options of CKGRACF USER PWSET"
- Scope access checks for CKGRACF USER
- Schedule access checks for CKGRACF USER SCHEDULE

Access checks for options of CKGRACF USER PWSET: The PWSET option can also have several sub-options. For backward compatibility, the PWSET option alone includes all sub-options in the command profile check. Therefore, for profile checking, the CKG.CMD.USER.*action-qual*.PWSET command is effectively the same as the CKG.CMD.USER.*action-qual*.PWSET.* command for checking.

A full list of checks is shown in the following table.

Table 6. Command access checks for CKGRACF USER subcommands

USER subcommand	Resource name checked	Access required
INTERVAL	CKG.CMD.USER.*action-qual*.INTERVAL	UPDATE
NOINTERVAL	CKG.CMD.USER.*action-qual*.NOINTERVAL	UPDATE

Table 6. Command access checks for CKGRACF USER subcommands (continued)

USER subcommand	Resource name checked	Access required
PHRESET	CKG.CMD.USER.*action-qual*.PHRESET	UPDATE
PWDEFAULT	CKG.CMD.USER.*action-qual*.PWDEFAULT	UPDATE
PWNOEXIT	CKG.CMD.USER.*action-qual*.PWNOEXIT	UPDATE
PWNOHIST	CKG.CMD.USER.*action-qual*.PWNOHIST	UPDATE
PWNORULE	CKG.CMD.USER.*action-qual*.PWNORULE	UPDATE
PWRESET	CKG.CMD.USER.*action-qual*.PWRESET	UPDATE
PWSET	CKG.CMD.USER.*action-qual*.PWSET	UPDATE
PWSET CURRENT	CKG.CMD.USER.*action-qual*.PWSET.CURRENT	UPDATE
PWSET DEFAULT	CKG.CMD.USER.*action-qual*.PWSET.DEFAULT	UPDATE
PWSET EXPIRED	CKG.CMD.USER.*action-qual*.PWSET.EXPIRED	UPDATE
PWSET NONEXPIRED	CKG.CMD.USER.*action-qual*.PWSET.NONEXP	UPDATE
PWSET NOPASSWORD	CKG.CMD.USER.*action-qual*.PWSET.NOPASSWORD	UPDATE
PWSET NOPHRASE	CKG.CMD.USER.*action-qual*.PWSET.NOPHRASE	UPDATE
PWSET NOPROTECTED	CKG.CMD.USER.*action-qual*.PWSET.NOPROTECTED	UPDATE
PWSET PASSWORD	CKG.CMD.USER.*action-qual*.PWSET.PASSWORD	UPDATE
PWSET PHRASE	CKG.CMD.USER.*action-qual*.PWSET.PHRASE	UPDATE
PWSET PREVIOUS	CKG.CMD.USER.*action-qual*.PWSET.PREVIOUS	UPDATE
PWSET PROMPT	CKG.CMD.USER.*action-qual*.PWSET.PROMPT	UPDATE
PWSET PROTECTED	CKG.CMD.USER.*action-qual*.PWSET.PROTECTED	UPDATE
PWSET RANDOM	CKG.CMD.USER.*action-qual*.PWSET.RANDOM	UPDATE
RESUME	CKG.CMD.USER.*action-qual*.RESUME	UPDATE
SCHEDULE	CKG.CMD.USER.*action-qual*.SCHEDULE	UPDATE

Table 7. Action-qualifiers in checked resource names

Action	Value for *action-qual*
ASK	ASK
REQUEST	REQ
WITHDRAW	REQ
SECOND	SEC
COMPLETE	CMP

USER subcommands

This section describes the subcommands supported by the USER command.

INTERVAL: The INTERVAL subcommand can be used to set the password and password phrase interval for a user. If this value is lower than the system-wide interval setting, then it becomes the effective interval setting. Otherwise, the value from the system-wide interval setting is used. If the value is omitted, the system-wide interval is used. The user's password and password phrase (if any) are not affected. The INTERVAL subcommand is mutually exclusive with the NOINTERVAL subcommand.

The INTERVAL subcommand has the following syntax:

```
INTERVAL[(value)]
value       The value for the password and phrase interval.
```

PWDEFAULT: The PWDEFAULT subcommand can be used to set or delete a user's default password or password phrase. This default value is used when the PWRESET, PHRESET, or PWSET DEFAULT command is issued. The default password and password phrase are subject to the syntax rules, the password or phrase history, and the new-password or new-phrase exits at the time of setting. The password or phrase is stored in encrypted form using the algorithm in effect at the time of setting.

The PWDEFAULT subcommand has the following syntax:

```
PWDEFAULT [options]
options      Any PWDEFAULT subcommand option; see the following table.
```

Table 8 shows the PWDEFAULT password options.

Table 8. Options for CKGRACF USER PWDEFAULT

Option	Description
DELETE	This keyword can be followed by the PASSWORD or PHRASE keyword to indicate which default value is to be deleted. If neither is specified, the default PASSWORD is deleted.
PASSWORD(*value*)	Set the default password to *value*. The parentheses and the value can be omitted for queued-command actions other than REQUEST.
PHRASE('*value*')	Set the default phrase to *value*. The parentheses, quotation marks, and the value can be omitted for queued-command actions other than REQUEST. Setting a default password phrase is supported only when the KDFAES password hashing algorithm is active.
PROMPT	This keyword can be followed by the PASSWORD or PHRASE keyword to indicate for which value the program prompts. If neither is specified, prompting is for the default PASSWORD. You are prompted twice to specify the required default value for the password or phrase. This option cannot be used in batch mode.

If no PWDEFAULT subcommand-option is specified, and the program is not running in batch mode, PROMPT is used. In batch mode, an error message is issued.

If the target userid is subject to multiple-authority controls, the program uses the value for the default password or phrase as specified with the original REQUEST. For subsequent actions, like COMPLETE APPROVE, any value specified for the PASSWORD or PHRASE subcommand is ignored.

If the default password is set while mixed case password support is inactive, and a password is reset (using CKGRACF) while mixed case password support is active, you might need to enter your password in uppercase to be able to logon.

If the PWDEFAULT subcommand is used in combination with the PWSET, PWRESET or PHRESET subcommands, the PWDEFAULT subcommand is run before the other subcommands. The other subcommands use the information as updated by the PWDEFAULT subcommand.

PHRESET: The PHRESET subcommand can be used to set the user's current password phrase to the user's default password phrase as set by CKGRACF. The function of this command is identical to PWSET DEFAULT PHRASE EXPIRED. The PHRESET subcommand is provided as a relatively safe option for a help desk, while the more powerful PWSET subcommand can be restricted.

The PHRESET subcommand has no parameters; it has the following syntax:

```
PHRESET
```

The PHRESET subcommand is mutually exclusive with the PWSET and PWRESET subcommands. If the target user is subject to multiple-authority controls, the default password phrase at the time of the REQUEST action is used. Changes to the default password phrase while the command is queued do not change the copy of the default password phrase stored with the queued command. If the default password phrase was changed during queueing, warning message CKG646I is issued when the command is completed. If no default password phrase can be found, the PHRESET subcommand fails; the user is not prompted for a password phrase.

If the PWDEFAULT for a PHRASE and the PHRESET subcommands are used in a single USER command, the PWDEFAULT subcommand is executed before the PHRESET subcommand.

PWSET: The PWSET subcommand can be used to set a user's password or password phrase.

It has the following syntax:

```
PWSET pwset-option expire-option
pwset-option      Any PWSET password option; see Table 9.
expire-option     Any PWSET expire option; see Table 10 on page 27.
```

The PWSET subcommand is mutually exclusive with the PWRESET and the PHRESET subcommands.

The *pwset-options* of the PWSET subcommand are:

Table 9. Options for CKGRACF USER PWSET

Option	Meaning
CURRENT	Leave the password and password phrase unchanged. This option is intended to be used in combination with the EXPIRED or NONEXPIRED keyword to expire or unexpire the current password or password phrase. The history values are not changed. If the CURRENT keyword is followed by the PHRASE keyword, the status of the password phrase is changed. In all other situations, the status of the password is changed.
DEFAULT	Set the password or password phrase to the default value. If the DEFAULT keyword is followed by the PHRASE keyword, the user's current password phrase is set. In all other cases, the user's current password is set. Resetting the current password phrase to a default value is supported only when the default password phrase has been set while the KDFAES password hashing algorithm was active.

Table 9. Options for CKGRACF USER PWSET (continued)

Option	Meaning
NOPASSWORD	Removes the ability for a user to logon using a password. This option requires that the userid already has a password phrase. If the user does not have a password phrase, a message is issued, and the command is rejected.
NOPHRASE	Removes the ability for a user to logon using a password phrase. This option requires that the userid already has a password. If the user does not have a password, a message is issued, and the command is rejected.
NOPROTECTED	Changes the user ID to a regular ID. This means that the user does not have the PROTECTED attribute. The user is no longer prevented from accessing the system using either a password or password phrase for authentication. You still need to assign a password or password phrase to the user ID.
PASSWORD*(value)*	Set the password to *value*, which is the password in clear text. The parentheses and value are optional if the action is not REQUEST.
PHRASE*(value)*	Set the password phrase to *value*, which is the password phrase in clear text, enclosed in single quotes. A single quote in the password phrase must be written as two consecutive single quotes, so a phrase like `th'is'phrase` must be specified as `'th''is''phrase'`. The parentheses and value are optional if the action is not REQUEST.
PREVIOUS	Reset the current password or password phrase to the previous value from the history. The current password or password phrase is added to the password history. Repeated use of the PWSET PREVIOUS subcommand alternates between two values, and does not travel back through the whole of the password or password phrase history. If the PREVIOUS keyword is followed by the PHRASE keyword, the password phrase is reset. In all other situations, the password is reset to the previous value.
PROMPT	Prompt and re-prompt for a password or password phrase. If the PROMPT keyword is followed by the PHRASE keyword, prompting is for a password phrase. In all other cases, prompting is for a password. This option cannot be used in a batch job.
PROTECTED	Changes the user ID to a protected ID. This means that the user can no longer access the system using either a password or password phrase for authentication. Any existing password or password phrase is removed and the PROTECTED attribute is assigned.
RANDOM	Set the password to a random string. See Creating random passwords.

If no *pwset-option* option is specified, DEFAULT PASSWORD is used. If no default password can be found, the user is prompted for a password. A new password specified for the PASSWORD or PROMPT options, or a prompted password for the DEFAULT option, is subject to the password rules, the password history, and the new-password exit.

When the default password is set while mixed case password support is inactive, and a password is reset (using CKGRACF) while mixed case password support is active, you might need to enter your password in uppercase to be able to logon.

If the PWDEFAULT and PWSET DEFAULT subcommands are used in a single USER command, the PWDEFAULT subcommand is executed before the PWSET subcommand.

If the target userid is subject to multiple-authority controls, the password or password phrase as read or specified in the REQUEST action is used. For subsequent actions, the PASSWORD option can be used with a dummy password or password phrase, and the PROMPT option does not prompt again. Changes to the default password while a PWSET DEFAULT subcommand is queued do not change the copy of the default password stored with the queued command; similarly, changes to the previous password while a PWSET PREVIOUS subcommand is queued do not change the copy of the previous password stored with the queued command. In both cases, warning message CKG645I or CKG646I is issued when the command is completed.

The PWSET expire options are:

Table 10. Expire options for CKGRACF USER PWSET

Option	Meaning
EXPIRED	Expire the new password or password phrase; it must be changed at the next logon.
NONEXPIRED	Do not expire the new password or password phrase.

If no expire option is specified, EXPIRED is used.

Chapter 4. zSecure CARLa Command Reference

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

SELECT/LIST Fields: RACF

These updates apply to zSecure Admin versions V2.1.0 and V2.1.1.

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(NOHIST) is in effect, RACF does not maintain a password history. In that case, the PWDHIST_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(NOHIST) 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

These updates apply to zSecure Admin versions V2.1.0 and V2.1.1.

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 Table 11 lists the possible values for this field. If the RACF Enhanced Password Encryption support is not installed, the field has the value LEGACY.

Table 11. Possible values for RACF_PWD_ALGORITHM

Value	Meaning
KDFAES	The KDFAES algorithm is used. This is a more secure encryption of the password and password phrase.
LEGACY	DES or the algorithm as 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. For details about allowed special characters, see the documentation in the *RACF Security Administrator's Guide*.

SELECT/LIST Fields: SYSTEM

These updates apply to zSecure Admin versions V2.1.0 and V2.1.1.

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 Table 12 lists the possible values for this field. If the RACF Enhanced Password Encryption support is not installed, the field has the value LEGACY.

Table 12. Possible values for RACF_PWD_ALGORITHM

Value	Meaning
KDFAES	The KDFAES algorithm is used. This is a more secure encryption of the password and password phrase.
LEGACY	DES or the algorithm as 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. For details about allowed special characters, see the documentation in the *RACF Security Administrator's Guide*.

Chapter 5. zSecure Command Verifier User Guide

This chapter lists the updates for the *IBM Security zSecure Command Verifier User Guide* as a result of the RACF password enhancement.

SETROPTS-related profiles

These updates apply to zSecure Command Verifier versions V1.12, V1.13.0, V1.13.1, V2.1.0, and V2.1.1.

In the table *Profiles used for verification of USER-related settings*, the following rows were added.

Table 13. Profiles used for verification of USER-related settings. The entries in this table reflect the SETROPTS keywords that are used to set a particular option.

Keyword	Value	Profile
PASSWORD	**ALGORITHM(KDFAES) NOALGORITHM**	**C4R.RACF.USER.PASSWORD.ALGORITHM**
PASSWORD	**(NO)SPECIALCHARS**	**C4R.RACF.USER.PASSWORD.SPECIALCHARS**

In the list that describes these profiles, the following entries were added:

- **C4R.RACF.USER.PASSWORD.ALGORITHM**

  This policy profile controls selecting the password encryption algorithm. The name of the selected ALGORITHM (KDFAES) is not represented in the zSecure Command Verifier policy profile.
- **C4R.RACF.USER.PASSWORD.SPECIALCHARS**

  This policy profile controls setting the option to allow additional special characters in user passwords.

Other user-related policy profiles

These updates apply to zSecure Command Verifier versions V1.12, V1.13.0, V1.13.1, V2.1.0, and V2.1.1.

In the table *Profiles used for user settings*, the following rows were added:

Table 14. Profiles used for user settings. The entries in this table reflect the keywords that are specified on the **ADDUSER** and **ALTUSER** commands

Command	Keyword	Profile
ALTUSER	**PWCLEAN**	**C4R.USER.PWCLEAN.***owner.userid*
ALTUSER	**PWCONVERT**	**C4R.USER.PWCONVERT.***owner.userid*

In the list that follows the table, the following entries were added:

- **C4R.USER.PWCLEAN.***owner.userid*

  This profile can be used to control cleanup of the password history for the user. The following access levels can be used for this policy profile:

No profile found
This control is not implemented. Any System-Special user can clean up the password and phrase history.

NONE
Cleanup of the password and phrase history is not allowed.

READ Same as NONE.

UPDATE
Cleanup of the password and phrase history is allowed. RACF still requires the terminal user to have the System-Special attribute.

CONTROL
The control is not implemented for this terminal user. RACF still requires the terminal user to have the System-Special attribute.

- **C4R.USER.PWCONVERT.***owner.userid*

This profile can be used to control conversion of the current password and history entries for the user. The following access levels can be used for this policy profile:

No profile found
This control is not implemented. Any System-Special user can convert the password and password history.

NONE
Conversion of the current password and password history is not allowed.

READ Same as NONE.

UPDATE
Conversion of the current password and password history is allowed. RACF still requires the terminal user to have the System-Special attribute.

CONTROL
The control is not implemented for this terminal user. RACF still requires the terminal user to have the System-Special attribute.

Chapter 6. zSecure Visual Client Manual

This chapter lists the updates for the *zSecure Visual Client Manual* as a result of the RACF password enhancement. These updates apply to zSecure Visual versions V2.1.0 and V2.1.1.

User Management

In the "User table" section, the following two columns were added:

LegacyPwdUsed
: This field indicates if the current user password is encrypted using a legacy algorithm. A legacy algorithm can either be DES or the algorithm as indicated by the ICHDEX01 password encryption exit (masking, DES, or installation-defined encryption method).

LegacyPwdCount
: This field indicates how many passwords in the password history are encrypted using a legacy algorithm.

Logging on

Users can now log on using either a password or a password phrase. Logging on using a password phrase requires PTF UA75331 (for V2.1.0) or UA75332 (for V2.1.1) to be installed on the zSecure Visual Server. zSecure Visual Server versions V1.12 and V1.13.*x* do not support logging on using a password phrase.

The password phrase can have a maximum length of 100 characters.

Chapter 7. 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 IBM Security zSecure versions V1.12, V1.13.0, V1.13.1, V2.1.0, and V2.1.1.

C4R755E Password history cleanup not allowed, command terminated

Explanation: This message is issued if a user with insufficient authority tries to perform the password and phrase history cleanup function. The user needs at least UPDATE access to the C4R.USER.PWCLEAN.*owner.user* policy profile.

C4R756E Password conversion not allowed, command terminated

Explanation: This message is issued if a user with insufficient authority tries to perform the current password and password history conversion function. The user needs at least UPDATE access to the C4R.USER.PWCONVERT.*owner.user* policy profile.

CKG113I Default password phrase set by *author* **at** *date time*

Explanation: This message indicates a default password phrase was set for the target user. It includes the user who issued the command and the date and time the default value was set. The default password phrase is not included in the message.

Severity: 00

CKG581I [New | Default] password phrase prepared for RRSF propagation

Explanation: This message notifies the user that CKGRACF concluded that a password synchronization package was in control and required password phrases to be passed in clear text. The only commands that can be synchronized are PWSET PHRASE and PWSET PASSWORD. Password phrases in queued PWSET PHRASE commands are two-way encrypted (hashed) with a fixed key. When such a command is being completed, its password phrase is decrypted and then sent as clear text with ENCRYPT=YES.

Severity: 00

CKG616I No default [password | password phrase] found - prompting

Explanation: This message indicates that a USER PWSET DEFAULT command or a USER PWSET DEFAULT PHRASE command was issued and no default password or password phrase was found. (This can be due to a USER PWDEFAULT DELETE command in the same USER command.) CKGRACF tries to prompt for a new password or password phrase. If this fails, message CKG618I is issued.

Severity: 00

CKG617I Prompting for default [password | password phrase] failed

Explanation: This message indicates that a USER PWDEFAULT PROMPT command or a USER PWDEFAULT PROMPT PHRASE command was issued. CKGRACF tried to prompt for a default password or password phrase, but this failed. This might be due to the user's profile settings, for example, PROFILE NOPROMPT. The USER command is not executed.

Severity: 08

CKG618I Prompting for [password | password phrase] failed

Explanation: This message indicates that a USER PWSET PROMPT command or a USER PWSET DEFAULT command was issued and no default password or password phrase was found. CKGRACF tried to prompt for a password or password phrase, but this failed. This might be due to the user's profile settings, for example, PROFILE NOPROMPT. The USER command is not executed.

Severity: 08

CKG619I Could not read previous [password | password phrase]

Explanation: This message indicates that a USER PWSET PREVIOUS command or a USER PWSET PREVIOUS PHRASE command was issued, but the previous password or password phrase could not be read because, for example, the previous password phrase was created when KDFAES was not in effect. The USER command is not executed.

Severity: 08

CKG635I Default [password | password-phrase] setting has a wrong format

Explanation: This message indicates that a

default-password or default-password-phrase setting was encountered that has a wrong format. This might indicate a defect in CKGRACF or that the USR field of the target user ID was altered by a different, incompatible command. Try to use the USER PWDEFAULT DELETE [PASSWORD | PHRASE] command to delete the incorrect setting from the target user ID. If the message refers to a password setting, you can also try to use the WIPE DEFAULTPW subcommand to delete the default password for the user ID. If the error occurs again, contact IBM Software Support.

Severity: 12

CKG645I Previous [password | password phrase] changed during queuing

Explanation: This warning message indicates that, during the execution of a queued USER PWSET PREVIOUS command, it was discovered that the previous password or password phrase was changed while the command was queued. The USER command uses the value of the previous password or password phrase from the time that the command was requested and first queued.

Severity: 04

CKG646I Default [password | password phrase] changed during queuing

Explanation: This warning message indicates that, during the execution of a queued USER PWSET DEFAULT, USER PWRESET, or USER PHRESET command, it was discovered that the default password or password phrase was changed or deleted while the command was queued. The USER command will use the value of the default password or password phrase from the time that the command was requested and first queued.

Severity: 04

CKG653I No default [password | password phrase] available

Explanation: A USER PWRESET or USER PHRESET command failed because no default password or password phrase was available. This can be due to a PWDEFAULT DELETE subcommand in the same USER command, or because no default password or password phrase is set for the target user.

Severity: 08

CKG655I RACF KDFAES enhancement not supported - upgrade to zSecure release 2.1.1 with APAR OA45989 necessary

Explanation: The current version of the CKGRACF program does not handle passwords and password phrases that have been hashed using the RACF KDFAES algorithm. Upgrade to zSecure 2.1.1 with the fix for APAR OA45989 installed. This provides a version of the CKGRACF program that supports the RACF KDFAES algorithm. This message only applies to z/OS V1.12 and above with the fix for APARs OA43998 and OA43999 installed.

User response: Upgrade to zSecure 2.1.1 with the fix for APAR OA45989 installed.

Severity: 12

CKG656I A `PWDX` change requires a `PASSWORD` change in the same `FIELD` command

Explanation: When a `FIELD` command with action ADD, SET, or REPLACE specifies a `PWDX` field, the same command must specify a `PASSWORD` field as well.

Severity: 12

CKG657I A `PHRASEX` change requires a `PHRASE` change in the same `FIELD` command

Explanation: When a `FIELD` command with action ADD, SET, or REPLACE specifies a `PHRASEX` field, the same command must specify a `PHRASE` field as well.

Severity: 12

CKG658I Field *field* is not allowed because `KDFAES` is not supported on this system

Explanation: This system does not support KDFAES. Therefore, fields `PWDX` and `PHRASEX` cannot occur in `FIELD` commands.

Severity: 12

CKG659I IRRSPW00: SAF RC (hex) *safrc*; RACF RC (hex) *racfrc*; RACF reason (hex) *racfreas*

Explanation: There was an error in callable service IRRSPW00. Contact IBM Software Support.

Severity: 24

CKG660I *PWSET option* option not allowed - use NOPROTECTED first

Explanation: The USER PWSET command cannot be used to change the password or password phrase of a protected user. Use the USER *userid* PWSET NOPROTECTED command to remove the protected status of the target user ID before changing the password or password phrase of the user.

Severity: 08

CKG684I [New | Default] password phrase contains more than 2 consecutive characters that are identical.

Explanation: The password phrase must not contain more than 2 consecutive characters that are identical.

Severity: 08

CKG685I [New | Default] password phrase must contain at least 2 alphabetic characters.

Explanation: The password phrase must contain at least 2 alphabetic characters, for example, A - Z or a - z.

Severity: 08

CKG686I [New | Default] password phrase must contain at least 2 non-alphabetic characters.

Explanation: The password phrase must contain at least 2 non-alphabetic characters, for example, numerics, punctuation, or special characters.

Severity: 08

CKG687I [New | Default] password phrase contains the user ID.

Explanation: The password phrase must not contain the user ID as sequential uppercase or sequential lowercase characters.

Severity: 08

CKG690I Could not encrypt [New | Default] password phrase for user *user*.

Explanation: A USER command for target user *user* was not executed, since the new password phrase could not be encrypted. Use DEBUG SAFRC to view the RACROUTE return codes; message CKG406I indicates the RACROUTE encryption return codes.

Severity: 08

CKG691I [New | Default] password phrase occurs in password phrase history.

Explanation: The new password phrase occurs in the password phrase history of the user. No new password phrase will be set.

Severity: 08

CKG692I [New | Default] password phrase not allowed by new-password-phrase exit.

Explanation: A new password phrase was not allowed by the installation's new-password-phrase exit ICHPWX11. The new password phrase will not be used.

Severity: 08

CKG694I [NOPASSWORD | NOPHRASE] option not allowed - add a [PHRASE | PASSWORD] first or use PROTECTED

Explanation: The `USER PWSET NOPASSWORD` command or the `USER PWSET NOPHRASE` command would create a user without a password and without a phrase.

User response: Either assign a value to the other field or make the user protected using the `USER PWSET` *`userid`* `PROTECTED` command.

Severity: 08

CKG697I Default password phrase can only be set when using the KDFAES algorithm.

Explanation: The PWDEFAULT PHRASE subcommand is only supported if the KDFAES password hashing algorithm is used. You can change the current password algorithm using the SETROPTS PASSWORD(ALGORITHM(KDFAES)).

Severity: 08

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 Contacting IBM Software Support 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 Contacting IBM Software Support to report the problem.

Severity: 24

Printed in USA