RACF Password Phrase Interval Support:
V1.00 APARs: RACF OA61951, SAF OA61952

Summary of Changes		
Version	**Date**	**Nature of Change**
V1.00	6/29/2022	Initial version

1 Introduction

Existing Support for Password Interval:
RACF installations can establish policy that a user's password or password phrase must be changed after a certain number of days. The security administrator can use the SETROPTS command to set the system level password interval with the PASSWORD(INTERVAL(n)) keywords. Additionally, each user can be given a shorter password and password phrase interval with the PASSWORD or PHRASE command and INTERVAL keyword.

New Support for Password Phrase Interval:
Support is added to RACF to provide a new separate password phrase specific change interval which can be different than the existing password interval and supports much longer values. The password phrase interval can be set with the new PHRASEINT keyword at the system level with the SETROPTS command and at the user level with the PASSWORD or PHRASE commands.

For more details on password phrase interval support, please refer to updated publication sections below.

Restriction: The ISPF panels are not updated for the new command operands with OA61951 and OA61952.

2 Planning
When installing service like this, consider the following before making changes:
- Create a backup copy of your RACF database.

- Apply the RACF Password Phrase APARs to all systems sharing the RACF database.

2.1 Create a backup copy of your RACF database

Creating a backup of the RACF database is recommended whenever significant changes are being made to RACF and the RACF database.

2.2 Apply the RACF Password Phrase Interval APARs to all systems that share the RACF database

Make sure that the service is applied on all sharing systems, and that all the ++HOLD documentation has been reviewed.

2.3 RACF exit considerations

The RACROUTE REQUEST=VERIFY preprocessing exit (ICHRIX01) and post processing exit (ICHRIX02) parameter list (RIXP) is updated to add the new password phrase interval user value. See the updated RACF Data Areas publication description for details.

Note that the existing RACF new-password exit (ICHPWX01) parameter list is not updated to add a parameter for the new password phrase interval. The existing RACF command exit (IRREVX01) includes all parameters specified on the PASSWORD and PHRASE commands including the new PHRASEINT keyword.

3 Updated RACF publications

Chapters of the following RACF publications are affected by the new function:

Publication Name	Publication Number
z/OS Security Server RACF Security Administrator's Guide	SA23-2289
z/OS Security Server RACF General User's Guide	SA23-2298
z/OS Security Server RACF Command Language Reference	SA23-2292
z/OS Security Server RACF Callable Services	SA23-2293
z/OS Security Server RACF RACROUTE Macro Reference	SA23-2294
z/OS Security Server RACF Macros and Interfaces	SA23-2288
z/OS Security Server RACF Data Areas	GA32-0885
z/OS Security Server RACF Messages and Codes	SA23-2291

In the following sections, highlighting is used to denote changed information in existing documentation. Sections, tables, messages, command keywords, etc. without highlighting contain new information.

3.1 z/OS Security Server RACF Security Administrator's Guide

This information supplements the following chapters:

- *Chapter: 'Specifying RACF options'*
  - *Section: SETROPTS options for initial setup*

3.1.1 Specifying RACF options

SETROPTS options for initial setup

…

Setting the maximum and minimum change interval (PASSWORD option)

If you have the SPECIAL attribute, you can specify the INTERVAL, PHRASEINT and MINCHANGE suboperands of the SETROPTS PASSWORD command. The INTERVAL suboperand specifies the system default for the maximum number of days that each user's password and password phrase remain valid. The PHRASEINT suboperand specifies the system default for the number of days that each user's password phrase remains valid and overrides the INTERVAL setting for password phrases. The MINCHANGE suboperand specifies the system default for the minimum number of days that must pass between a user's password (and password phrase) changes. The following example specifies that each user's password ~~and password phrase~~ remain valid for 60 days (as long as the system default for these users remains 60 days), specifies that each user's password phrase remain valid for 365 days and that no user can change their password or password phrase more often than every 30 days (as long as the system default for these users remains 30 days).

```
SETROPTS PASSWORD(INTERVAL(60) PHRASEINT(365) MINCHANGE(30))
```

These values become effective immediately as:

- The default ~~values~~ password change interval for new users whom you define to RACF through the ADDUSER command
- The upper limit for users who specify the INTERVAL operand on the PASSWORD command
- The effective password phrase interval for users who do not have a user specific phrase interval value set in their user profile.

The initial system default is 30 days for the maximum change interval (INTERVAL) and 0 days for minimum change interval (MINCHANGE). The value MINCHANGE(0) allows users to change their passwords and password phrases more than once each day.
The initial default for the password phrase interval (PHRASEINT) is 0 which indicates that the INTERVAL keyword is used to control the password phrase interval.
When users are defined to RACF and have access to the system, they can use the INTERVAL operand of the PASSWORD command to set their own change interval to a value less than 30 or to a value less than that which you specified on the INTERVAL

operand of the SETROPTS command (if you did so).

Restrictions:

1. When you change the SETROPTS PASSWORD(INTERVAL) value, the password interval set in each user's profile is not changed. If a user's INTERVAL value in the user's profile (as set using the PASSWORD command) is different than the SETROPTS value, RACF expires the password or password phrase at the shorter interval of the two values.
2. When you change the SETROPTS PASSWORD(PHRASEINT) value, a password phrase interval set in each user's profile is not changed. When a user does not have a PHRASEINT value set the SETROPTS PHRASEINT value is used. When the user has a PHRASEINT value set it overrides the SETROPTS PHRASEINT value.
3. Avoid setting the MINCHANGE value higher than any individual user's INTERVAL value (as set using the PASSWORD command). If you do, RACF expires the user's password or password phrase when the MINCHANGE period elapses, not when the user's INTERVAL elapses. Users cannot change their own passwords or password phrases until the MINCHANGE period elapses, even when the user's INTERVAL value defines a shorter period than the MINCHANGE value.

User consideration: Users who attempt to change their passwords or password phrases before the minimum change interval elapses are notified of their change failures but are not notified of the reason. The reason for the failure is withheld in the event of unethical user behavior, particularly by outside users or hackers who might exploit the information.

3.2 z/OS Security Server RACF General User's Guide

This information supplements the following chapters and sections:

- *Chapter: 'Changing how you are defined to RACF'*
  - *Section: 'Changing your password'*
  - *Section: 'Changing your password phrase'*

3.2.1 Changing your password

This section is updated to include details regarding the new password phrase interval control.

To change your password interval (that is, the time allowed before you are required to change your password again), enter the PASSWORD command with the INTERVAL keyword as follows:

```
PASSWORD INTERVAL(interval-you-want)
```

For example, to change your password interval to 15 days, enter the following command:

```
PASSWORD INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password.
RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you can change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.
If you do not know your current password interval, enter the LISTUSER command and check the PASSINTERVAL field. For more information, see "Understanding the information RACF has about you as a user".

To change your password and password interval, enter the PASSWORD command with the PASSWORD and INTERVAL keywords as follows:

```
PASSWORD PASSWORD(current-password new-password) INTERVAL(interval)
```

For example, to change the password from "subject" to "testers", and the interval to 15 days, enter the following command:

```
PASSWORD PASSWORD(subject testers) INTERVAL(15)
```

Note: Installations can also set a separate system password phrase interval value. In this case, the PASSWORD/PHRASE command INTERVAL keyword no longer controls the password phrase interval. An administrator can use the PASSWORD/PHRASE command PHRASEINT keyword to override a user's password phrase interval.

3.2.2 Changing your password phrase

This section is updated to include details regarding the new password phrase interval control.

To change your password phrase, enter the PASSWORD or PHRASE command with the PHRASE keyword as follows:

```
PASSWORD PHRASE ('current-password-phrase' 'new-password-phrase')
```

or

```
PHRASE PHRASE ('current-password-phrase' 'new-password-phrase')
```

The current and new password phrases must have different values. Note that the password phrases must be entered in quotation marks. TSO/E does not support entering quoted strings in print inhibit mode; therefore your password phrase is visible on the display. Take care to ensure that nobody can view your password phrase.
For example, to change your password phrase from "December 27, 1950" to "In 1492 Columbus sailed the ocean blue", type:

```
PASSWORD PHRASE ('December 27, 1950' 'In 1492 Columbus sailed the ocean blue')
```

or

```
PHRASE PHRASE ('December 27, 1950' 'In 1492 Columbus sailed the ocean blue')
```

The password interval (that is, the time allowed before you are required to change your password again) also applies to the password phrase. For a description of how to change the password interval, see “Changing your password”. You can use either the PASSWORD or PHRASE command. For example, to change your password interval to 15 days, enter either of the following commands:

```
PASSWORD INTERVAL(15)
```

or

```
PHRASE INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password phrase.

Note: Installations can also set a separate system password phrase interval value. In this case, the PASSWORD/PHRASE command INTERVAL keyword no longer controls the password phrase interval. An administrator can use the PASSWORD/PHRASE command PHRASEINT keyword to override a user’s password phrase interval.

3.3 z/OS Security Server RACF Command Language Reference

This information supplements the following chapters and sections:

- *Chapter: 'RACF Command Syntax'*
  - *Section: LISTUSER*
  - *Section: PASSWORD or PHRASE*
  - *Section: SETROPTS*

3.3.1 LISTUSER

The LISTUSER command is updated to list the phrase interval.

Purpose

…
The details RACF lists from the BASE segment for each user profile are:

…

- The change interval (in number of days)
- The password phrase change interval (in number of days)

…

Details about listing the password and password phrase change interval:

Users will always have a password interval but may or may not have a password phrase interval value. When a user does not have a password phrase interval value set the password interval value is used as both the password interval and password phrase interval. In this case, LISTUSER will not list the user's PHRASE INTERVAL value.

…

Examples

…

```
LISTUSER
USER=DAF0 NAME=D.M.BROWN OWNER=IBMUSER CREATED=05.228
DEFAULT-GROUP=RESEARCH PASSDATE=05.228 PASS-INTERVAL= 30 PHRASEDATE=05.231
PHRASE-INTERVAL=00365
PASSWORD ENVELOPED=NO
ATTRIBUTES=ADSP
ATTRIBUTES=PASSPHRASE
REVOKE DATE=NONE RESUME DATE=NONE
LAST-ACCESS=05.228/13:31:11
CLASS AUTHORIZATIONS=NONE
```

```
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED (DAYS) (TIME)
------------------------------------------
ANYDAY ANYTIME
GROUP=RESEARCH AUTH=JOIN CONNECT-OWNER=IBMUSER CONNECT-DATE=05.228
CONNECTS= 01 UACC=READ LAST-CONNECT=05.228/13:31:11
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
GROUP=PAYROLLB AUTH=CREATE CONNECT-OWNER=IBMUSER CONNECT-DATE=05.228
CONNECTS= 00 UACC=READ LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
```

Figure 19. Example 1: Output for LISTUSER

3.3.2 PASSWORD or PHRASE (Specify user password or password phrase)

The PASSWORD and PHRASE commands are updated to add the new PHRASEINT password phrase interval keyword.

Syntax

[subsystem-prefix]{PASSWORD | PW | PHRASE}
[AT([node].userid ...) | ONLYAT([node].userid ...)]
[INTERVAL(change-interval) | NOINTERVAL]
[PHRASEINT(phrase-change-interval) | NOPHRASEINT]
[PASSWORD(current-password new-password)]
[PHRASE('current-password-phrase' 'new-password-phrase')]
[USER(userid ...)]

Parameters

…

INTERVAL | NOINTERVAL

INTERVAL(change-interval)

Specifies the number of days during which a user's password and password phrase (if set) remain valid; the value must be 1 - 254 days.

The INTERVAL value you specify here cannot exceed the system value (if any) that your installation specified using the INTERVAL operand on the SETROPTS command. (The initial system default after RACF initialization is 30 days.)

The INTERVAL value you specify should not be less than the value (if any) that your installation specified using the MINCHANGE operand on the SETROPTS command. If this occurs, the user's password and password phrase (if set) cannot expire until your installation's minimum interval is reached and the user will not be allowed to change them prior to expiration.

If you specify INTERVAL on the PASSWORD command without a change-interval value, RACF uses the system interval value (if any) that your installation specified or the system default.

To specify INTERVAL with USER, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

If you specify the interval incorrectly, RACF ignores this operand.

Note: The INTERVAL setting is overridden for password phrases in the following cases:

1) The user has a non-zero PHRASEINT value
2) The user has NOPHRASEINT
3) The system has a non-zero PHRASEINT value

NOINTERVAL

Specifies that neither a user's password nor password phrase (if set) will expire. To specify NOINTERVAL with USER, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Specifying NOINTERVAL without USER defines your own password and password phrase (if set) to never expire.

You can use INTERVAL at any time to reinstate an expiration interval for a user previously defined with NOINTERVAL.

Note: The NOINTERVAL setting is overridden for password phrases in the following cases:

1) The user has a non-zero PHRASEINT value
2) The user has NOPHRASEINT
3) The system has a non-zero PHRASEINT value

PHRASEINT | NOPHRASEINT

PHRASEINT(phrase-change-interval)

Specifies the number of days during which a user's password phrase remains valid; the value must be 0 – 65534 days.

A PHRASEINT value of 0 is the default value and indicates that the user does not have a specific password phrase interval value. In this case, when the system PHRASEINT is set to a non-zero value, that value is this user's effective password phrase interval. When the user PHRASEINT and system level PHRASEINT are set to 0 the user's INTERVAL value and system INTERVAL values are used to determine their password phrase interval.

The PHRASEINT value you specify can exceed the system value (if any) that your installation specified using the PHRASEINT or INTERVAL operand on the SETROPTS command.

The PHRASEINT value you specify should not be less than the value (if any) that your installation specified using the MINCHANGE operand on the SETROPTS command. If this occurs, the user's password phrase cannot expire until your installation's minimum interval is reached and the user will not be allowed to change them prior to expiration.

To specify PHRASEINT, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

If you specify the password phrase interval incorrectly, RACF ignores this operand.

NOPHRASEINT

Specifies that a user's password phrase will not expire.

To specify NOPHRASEINT with USER, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Specifying NOPHRASEINT without USER defines your own password phrase (if set) to never expire.

You can use PHRASEINT at any time to reinstate an expiration interval for a user previously defined with NOPHRASEINT.

3.3.3 SETROPTS (Set RACF options)

A new PHRASEINT keyword is added to the SETROPTS command to set the system password phrase interval.

Syntax

…
[PASSWORD(
[ALGORITHM(KDFAES) | NOALGORITHM]
[HISTORY(number-previous-values) | NOHISTORY]
[INTERVAL(maximum-change-interval)]
[MINCHANGE(minimum-change-interval)]
[MIXEDCASE | NOMIXEDCASE]
[PHRASEINT(password-phrase-change-interval)]
[REVOKE(number-incorrect-attempts) | NOREVOKE]
[{RULEn(LENGTH(m1:m2) content-keyword (position))
| NORULEn
| NORULES}]
[SPECIALCHARS | NOSPECIALCHARS]
[WARNING(days-before-expiration) | NOWARNING]
)]
…

PASSWORD(suboperands)

Specifies options to monitor and check passwords and password phrases:

…

INTERVAL(maximum-change-interval)

Specifies the maximum number of days (1 - 254) each user's password and password phrase are valid. For example, if you specify 90 for your INTERVAL number, each user's password is valid for 90 days and each user's password phrase (if set) is valid for 90 days.

RACF uses the value you specify for maximum-change-interval as both:

• The default value for new users defined to RACF through the ADDUSER command.

• The upper limit for users who specify the INTERVAL operand on the PASSWORD command.

When a user logs on to the system, RACF compares this INTERVAL value (the system interval) with the interval value specified in the user's profile (the user's interval). RACF uses the lower of the two values to determine if the user's password and password phrase have expired.

The initial default at RACF initialization is 30 days. The maximum change interval cannot be less than the minimum change interval set with the MINCHANGE keyword.

When the system password phrase interval is set to zero the password interval is also used as the password phrase interval. In this case the following line is displayed from a SETROPTS LIST:

```
PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
```

Note: The INTERVAL setting is overridden for password phrases in the following cases:

1) The user has a non-zero PHRASEINT value
2) The user has NOPHRASEINT
3) The system has a non-zero PHRASEINT value

…

PHRASEINT(password-phrase-change-interval)

Specifies the default number of days (0 - 65534) each user's password phrase is valid. For example, if you specify 365 for your PHRASEINT number, each user's password phrase is valid for 365 days.

The default PHRASEINT value is 0 which indicates that the system does not have a password phrase interval value. In this case, when the user PHRASEINT is set to a non-zero value, that value is this user's effective password phrase interval. When both the system PHRASEINT value and the user level PHRASEINT are set to 0 the shorter of either the user's INTERVAL value or the system INTERVAL is used as the effective password phrase interval.

When the system password phrase interval is set to zero the following line is displayed from a SETROPTS LIST:

```
PASSWORD CHANGE INTERVAL IS IN EFFECT FOR PASSWORD PHRASES.
```

When a user logs on to the system, RACF compares this PHRASEINT value (the system interval) with the interval value specified in the user's profile (the user's interval). When a user has a nonzero PHRASEINT value that value is used as their password phrase interval. When a user has a user PHRASEINT value of 0 the system level PHRASEINT value is used as their password phrase interval.

The password phrase change interval cannot be less than the minimum change interval set with the MINCHANGE keyword.

…

EXAMPLES

…

```
SETROPTS LIST
```

```
ATTRIBUTES = INITSTATS NOWHEN(PROGRAM) TERMINAL(READ) SAUDIT
CMDVIOL NOOPERAUDIT
STATISTICS = DATASET AIMS APPL DASDVOL GCICSTRN GIMS PCICSPSB
QCICSPSB TAPEVOL
TCICSTRN TERMINAL TIMS
AUDIT CLASSES = DATASET USER GROUP AIMS APPL DASDVOL GCICSTRN GIMS
PCICSPSB QCICSPSB TAPEVOL TCICSTRN TERMINAL TIMS
ACTIVE CLASSES = DATASET USER GROUP ACICSPCT AIMS APPL BCICSPCT
CCICSCMD DASDVOL
DCICSDCT ECICSDCT FCICSFCT GCICSTRN GIMS GLOBAL GMBR HCICSFCT
JCICSJCT KCICSJCT MCICSPPT NCICSPPT PCICSPSB QCICSPSB RACGLIST
SCICSTST TAPEVOL TCICSTRN TERMINAL TIMS UCICSTST VCICSCMD VMRDR
VMMDISK
GENERIC PROFILE CLASSES = DATASET ACICSPCT AIMS APPL CCICSCMD
DASDVOL DCICSDCT
FCICSFCT GMBR JCICSJCT MCICSPPT PCICSPSB SCICSTST
TAPEVOL TCICSTRN TERMINAL TIMS VMBATCH VMCMD VMMDISK
VMNODE VMRDR
GENERIC COMMAND CLASSES = DATASET ACICSPCT AIMS APPL CCICSCMD
DASDVOL DCICSDCT
FCICSFCT GMBR JCICSJCT MCICSPPT PCICSPSB SCICSTST
TAPEVOL TCICSTRN TERMINAL TIMS VMBATCH VMCMD VMMDISK
VMNODE VMRDR
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = VMMDISK
SETR RACLIST CLASSES = ACCTNUM DASDVOL
GLOBAL=YES RACLIST ONLY = JCICSJCT TCICSTRN
LOGOPTIONS "ALWAYS" CLASSES = DASDVOL GDASDVOL SECLABEL
LOGOPTIONS "NEVER" CLASSES = FACILITY VMXEVENT VXMBR
LOGOPTIONS "SUCCESSES" CLASSES = APPCLU RACFVARS RVARSMBR
LOGOPTIONS "FAILURES" CLASSES = DATASET PMBR PROGRAM PROPCNTL
LOGOPTIONS "DEFAULT" CLASSES = GTERMINL TAPEVOL TERMINAL
AUTOMATIC DATASET PROTECTION IS IN EFFECT
ENHANCED GENERIC NAMING IS IN EFFECT
REAL DATA SET NAMES OPTION IS ACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
```



```
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL OPTION IS NOT IN EFFECT
TAPE DATA SET PROTECTION IS ACTIVE
SECURITY RETENTION PERIOD IN EFFECT IS 365 DAYS
ERASE-ON-SCRATCH IS INACTIVE
SINGLE LEVEL NAME PREFIX IS RDSPRFX
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
DATA SET MODELLING NOT BEING DONE FOR GDGS.
USER DATA SET MODELLING IS BEING DONE.
GROUP DATA SET MODELLING IS BEING DONE.
PASSWORD PROCESSING OPTIONS:
   THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
   PASSWORD CHANGE INTERVAL IS 254 DAYS.
   PASSWORD PHRASE CHANGE INTERVAL IS   365 DAYS.
   PASSWORD MINIMUM CHANGE INTERVAL IS 2 DAYS.
   MIXED CASE PASSWORD SUPPORT IS IN EFFECT.
   SPECIAL CHARACTERS ARE ALLOWED.
   13 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
   AFTER 4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS, A USERID
   WILL BE REVOKED.
   PASSWORD EXPIRATION WARNING LEVEL IS 186 DAYS.
   INSTALLATION PASSWORD SYNTAX RULES:
   RULE 1 LENGTH(4:5) LLLLL
   RULE 2 LENGTH(5) AAAAA
   RULE 3 LENGTH(6:8) LLLLLLLL
   RULE 4 LENGTH(6:8) NNNNNNNN
   RULE 5 LENGTH(6:8) AAAAAAAA
   LEGEND:
   A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
   ANYTHING
   c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-
   SPECIAL x-MIXEDALL
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
```

```
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
SECLEVELAUDIT IS INACTIVE
SECLABEL AUDIT IS IN EFFECT
SECLABEL CONTROL IS IN EFFECT
GENERIC OWNER ONLY IS IN EFFECT
COMPATIBILITY MODE IS IN EFFECT
MULTI-LEVEL QUIET IS IN EFFECT
MULTI-LEVEL STABLE IS IN EFFECT
NO WRITE-DOWN IS IN EFFECT. CURRENT OPTIONS:
"MLS WARNING" OPTION IS IN EFFECT
MULTI-LEVEL SECURE IS IN EFFECT. CURRENT OPTIONS:
"MLS WARNING" OPTION IS IN EFFECT
MULTI-LEVEL ACTIVE IS IN EFFECT. CURRENT OPTIONS:
"MLACTIVE FAIL" OPTION IS IN EFFECT
CATALOGUED DATA SETS ONLY, IS IN EFFECT. CURRENT OPTIONS:
"CATDSNS WARNING" OPTION IS IN EFFECT
USER-ID FOR JES NJEUSERID IS : ????????
USER-ID FOR JES UNDEFINEDUSER IS : ++++++++
PARTNER LU-VERIFICATION SESSIONKEY INTERVAL MAXIMUM/DEFAULT IS 30
days
APPLAUDIT IS IN EFFECT
ADDCREATOR IS IN EFFECT
KERBLVL = 0
MULTI-LEVEL FILE SYSTEM IS IN EFFECT
MULTI-LEVEL INTERPROCESS COMMUNICATIONS IS IN EFFECT
MULTI-LEVEL NAME HIDING IS NOT IN EFFECT
SECURITY LABEL BY SYSTEM IS NOT IN EFFECT
PRIMARY LANGUAGE DEFAULT : ENU / AMERICAN
SECONDARY LANGUAGE DEFAULT : ENU / AMERICAN
```


3.4 z/OS Security Server RACROUTE Macro Reference

This information supplements the following chapters and sections:

- *Chapter: 'Appendix B. RACF database templates'*
  - *Section: 'User template'*

3.4.1 User template

The user template is updated to add the new phrase interval field.

Template							**Field being described**
Field name	**Field ID**	**Flag 1**	**Flag 2**	**Field length dec**	**Default value**	**Type**	
The following is the BASE segment of the USER template.							
…							
PASSINT	011	00	80	00000001	FF	Int	The interval in days (represented by a number between 1 and 254) that the user's password is in effect. If it is X'FF', the user's password never expires. See the description of the SETR PASSWORD(INTERVAL...)) processing instructions in z/OS Security Server RACF Command Language Reference for more details.
…							
MFAPOLNM	121	80	80	00000000	00		Policy name - repeat
PHRINT	122	00	80	00000002	00	Int	The password change interval in days (represented by a number between 0 and 65534) that the user's password phrase is in effect. If it is X'FFFF', the user's password phrase never expires. See the description of the SETR PASSWORD (PHRASEINT...)) processing instructions in z/OS Security Server RACF Command Language Reference for more details.

3.5 z/OS Security Server RACF Callable Services

This information supplements the following chapters and sections:

- *Chapter: 'Appendix B. Reference documentation tables'*
  - *Section: 'User administration'*
  - *Section: 'SETROPTS administration'*

3.5.1 User administration

The R_admin reference appendix is updated to add new fields to the user administration table 'BASE segment fields' as follows:

BASE segment fields:

Field name	SAF field name	Flag byte value	RDEFINE/RALTER keyword reference	Allowed on add requests	Allowed on alter requests	Returned on extract requests
…						
PHRDATE		N/A	PHRASEDATE=	No	No	Yes
PHRINT		N/A	PHRASE INTERVAL=	No	No	Yes
PPHENV (boolean)		N/A	PHRASE ENVELOPED=	No	No	Yes
…						

3.5.2 SETROPTS administration

The R_admin reference appendix is updated to add new fields to the SETROPTS administration table 'BASE segment field names' as follows:

BASE segment field names:

Field name	Flag byte value	SETROPTS keyword reference
…		
OPERAUDT (boolean)	'Y'	OPERAUDT
	'N'	NOOPERAUDT
PHRINT	'Y'	PASSWORD (PHRASEINT(xx))
PREFIX	'Y'	PREFIX(xx)
	'N'	NOPREFIX

…		

3.6 z/OS Security Server RACF Macros and Interfaces

This information supplements the following chapters and sections:

- *Chapter: 'RACF database unload'*
  - *Section: 'Record formats produced by the database unload utility'*
- *Chapter: 'SMF records'*
  - *Section: 'Table of data type 6 command-related data'*
- *Appendix: 'RACF database templates'*
  - *Section: User template for the RACF database*

3.6.1 Record formats produced by the database unload utility

The User basic data record (0200) is updated to add a new field for the password phrase interval.

Field Name	Type	Start	End	Comments
USBD_RECORD_TYPE	Int	1	4	Record type of the User Basic Data record (0200)
…				
USBD_MFA_FALLBACK	Char	639	642	This user can use a password or password phrase to logon to the system when MFA is unavailable. Valid Values include "Yes" and "No".
USBD_PHR_INTERVAL	Char	644	648	The number of days that the user's password phrase can be used. Note: Users without a password phrase interval will have the value 0. Users with a non-expiring password phrase interval (NOPHRASEINT) will have the value 65535 (x'FFFF').

3.6.2 Record type 80: RACF processing record

Table of data type 6 command-related data

The "Table of data type 6 command-related data" is updated to add a new field for the password phrase interval to the PASSWORD and SETROPTS commands.

Event Code Dec(hex)	Command	Data length	Format	Description
…				

<table>
<tr><td>18(12)</td><td>PASSWORD</td><td>1</td><td>mixed</td><td>Flags for keywords specified<table><tr><th>Bit</th><th>Keyword specified</th></tr><tr><td>0</td><td>INTERVAL</td></tr><tr><td>1</td><td>USER</td></tr><tr><td>2</td><td>PASSWORD</td></tr><tr><td>3</td><td>PHRASE</td></tr><tr><td>4</td><td>PHRASEINT</td></tr><tr><td>5-7</td><td>Reserved for IBM’s use</td></tr></table></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>8</td><td>EBCDIC</td><td>UserID (USER keyword)</td></tr>
<tr><td></td><td></td><td>4</td><td>Binary</td><td>Password phrase change-interval (PHRASEINT keyword)
Note: If the NOPHRASEINT keyword is specified, the Password phrase change-interval changes to 65535 (x'FFFF').</td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td></tr>
<tr><td>24(18)</td><td>SETROPTS</td><td>4</td><td>Binary</td><td>Flags for keywords specified<table><tr><th>Bit</th><th>Keyword specified</th></tr><tr><td>0</td><td>Primary language specified</td></tr><tr><td>…</td><td></td></tr><tr><td>14</td><td>Password NOALGORITHM specified</td></tr><tr><td>15</td><td><s>Reserved for IBM's use</s>
Password PHRASEINT specified</td></tr><tr><td>16</td><td>MLFSOBJ(ACTIVE) specified</td></tr></table></td></tr>
<tr><td>…</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td>1</td><td>Binary</td><td>Password algorithm in effect<table><tr><th>Bit</th><th>Meaning</th></tr><tr><td>0</td><td>Existing algorithm as indicated by ICHDEX01 (masking, DES, or installation-defined)</td></tr><tr><td>1</td><td>KDFAES</td></tr></table></td></tr>
<tr><td></td><td></td><td>2</td><td>Binary</td><td>Password Phrase change-interval (PHRASEINT keyword)</td></tr>
<tr><td></td><td></td><td><s>75</s>
73</td><td>EBCDIC</td><td>Reserved for IBM's use</td></tr>
</table>

3.6.3 Record type 81: RACF initialization record

The RACF initialization record is updated to add a new field for the password phrase interval.

RACF writes record type 81 at the completion of the initialization of RACF. This record contains:

- Record type
- Time stamp (time and date)
- Processor identification
- Name of each RACF database
- Volume identification of each RACF database
- Unit name of the RACF database
- Data set name of the UADS data set
- Volume identification of the UADS data set
- RACF options
- The maximum password interval
- The password phrase interval
- The default installation language codes in effect at IPL time.

The format of record type 81 is:

Initialization Record (type 81)

Offsets					
Dec.	**Hex.**	**Name**	**Length**	**Format**	**Description**
…					
181	B5	SMF81VXA	8	EBCDIC	VMXEVENT audit profile is in effect
198	C6	SMF81PHI	2	Binary	Password phrase interval
200	C8		~~57~~ 55	Reserved.	
…					

3.6.4 Record type 81: The format of the unloaded SMF type 81 data

The RACF initialization record is updated to add a new field for the password phrase interval.

Format of the unloaded SMF type 81 records

Field Name	Type	Len	Start	End	Comments
RINI_EVENT_TYPE	Char	8	1	8	The type of the event. Set to "RACFINIT".
…					
RINI_PWD_ALG	Char	10	766	777	Algorithm that is used to encrypt passwords and password phrases. Possible values are "KDFAES" and "LEGACY".
RINI_ENHANCED_GENOWNER	Yes/No	4	779	782	Is ENHANCEDGENERICOWNER in effect?
RINI_PHR_INT	Integer	5	784	788	The password phrase interval.

3.6.5 RACF database templates

The BASE segment is updated in the USER section to add a new field for password phrase interval.

```
$/TEMPLATE 002 USER VERSION 1'
$/SEGMENT  001 BASE'
...
MFAPOLNM 121 80 80 00000000 00 MFA - Policy name - repeat
PHRINT   122 00 80 00000002 00 Phrase change interval
...
```

The RACF templates version is updated to:

```
VERSION OA61951 00000243.00000060
```

3.7 z/OS Security Server RACF Data Areas

This information supplements the following chapter and sections:

- *Chapter: 'RACF Data Areas'*
  - *Section: RCVT: RACF Communication Vector Table*
  - *Section: RIXP: RACROUTE REQUEST=VERIFY/VERIFYX Exit Parameter List*

3.7.1 RCVT: RACF Communication Vector Table

The RCVT: RACF Communication Vector Table adds two new fields:

1. The RCVTPHIN field indicates the system setting for the password phrase interval. A value of 0 indicates that a system level password phrase interval value is not set and the RCVTPINV value should be used as the system password phrase interval.
2. The RCVTPHIA field indicates that the password phrase interval functions are available. Other products can check this field to determine if the current version of RACF has enhanced PassTicket support added either in the base OS or via PTF.

Offset (dec)	Offset (Hex)	Type	Len	Name(Dim)	Description
…					
155	9B	ADDRESS	1	RCVTPINV	GLOBAL MAX PASSWORD INTERVAL VALUE - VALID RANGE 1-254. This field is also used as the system password phrase interval unless the RCVTPHIN field has a non-zero value.
...					
496	1F0	ADDRESS	4	RCVTMXPW	Address of enhanced password routine (IRRMXPW0)
500	1F4	UNSIGNED	2	RCVTPHIN	Password phrase interval – valid range 0-65534. When set to a non-zero value, this field is used as the system password phrase interval. Otherwise, the RCVTPINV value should be used as the system password phrase interval.
502	1F6	CHARACTER	94	*	Reserved
...					
640	280	BITSTRING	1	RCVTFLG4	Function availability bits
...					
	.... 1...			RCVTPHIA	Phrase interval Functions (OA61951)

					are available.
...					

3.7.2 RIXP: RACROUTE REQUEST=VERIFY/VERIFYX Exit Parameter List

The RIXP: RACROUTE REQUEST=VERIFY/VERIFYX Exit Parameter List Table adds one new field for the user's phrase interval.

Offset (dec)	Offset (Hex)	Type	Len	Name(Dim)	Description
…					
204	(CC)	ADDRESS	4	RIXIDTA	IDTA ADDRESS: points to an IDTA data area as mapped by IRRPIDTA.
208	(D0)	ADDRESS	4	RIXPHIA	Password Phrase Change Interval Address: points to a 4-byte area that contains a 31-bit fixed binary integer that represents the password phrase change interval value found in the user's profile. NOTE: Upon initial entry to exit ICHRIX01 the four byte field contains zeros. Upon entry to the ICHRIX02 exit, the four byte field contains the value from the user entry. Changes to this value are ignored by RACINIT processing.

3.8 z/OS Security Server RACF Messages and Codes

This information supplements the following chapter and section:

- *Chapter: 'ICH messages for RACF commands'*
  - *Section: 'SETROPTS command messages'*
  - *Section: 'PASSWORD command messages'*
- *Chapter: 'IRR messages for commands, utilities, and other tasks'*
  - *Section: 'RRSF handshaking messages'*

3.8.1 SETROPTS command messages

The message ICH14086I is added.

ICH14086I Minimum change interval exceeds the password phrase interval.

Explanation
The value specified for MINCHANGE exceeds the installation-specified maximum set by SETR PASSWORD(PHRASEINT).

System action
RACF ignores the operand and continues command processing with the next operand.

RACF Security Administrator Response
Issue SETR LIST to check the current minimum and maximum values and specify correct values.

3.8.2 PASSWORD command messages

The explanation for message ICH08007I is updated and message ICH08029I is added.

ICH08007I NOT AUTHORIZED TO CHANGE PASSWORD/INTERVAL FOR userid
Explanation
You are not allowed to change the password, ~~or~~ password interval, password phrase or password phrase interval for the user indicated in the message.
System action
The password, password interval, password phrase or password phrase interval is not changed.
User response
See your RACF security administrator.

ICH08029I PHRASEINT NOT IN RANGE 0-65534

Explanation
The password phrase change-interval must be at least 0 and no greater than 65534.

System action
The password phrase interval is not changed.

3.8.3 RRSF handshaking messages

The message IRRI007I text is updated to reflect the existing insert for different SETROPTS PASSWORD(options). The message may also include new insert text to indicate that the RRSF partner node password phrase interval setting is different than the local node.

IRRI007I ATTENTION: LOCAL NODE localnode HAS A DIFFERENT SETROPTS PASSWORD(option ~~RULEx~~) THAN PARTNER NODE partnernode.

Explanation
This is a warning message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. This message is issued when a difference is detected between the local node and partner node settings for the SETROPTS PASSWORD(options) for HISTORY, INTERVAL, PHRASEINT and RULEx.

When a SETROPTS PASSWORD(RULEx) option mismatch is detected, a change in password may be accepted on one node but rejected on the other node unless the SETROPTS password rules match. When the password rules are the same, they do not need to be listed in the same order on both nodes.

System action
If no error messages are issued with this warning message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I indicates when the OPERATIVE ACTIVE state is reached.

System programmer response
Evaluate the SETROPTS PASSWORD(option) that is listed in the message. These SETROPTS options must match when you want two RACF nodes to communicate with each other. You should use the SETROPTS PASSWORD(option) command to change one or both nodes so that the SETROPTS PASSWORD(options) match. When the SETROPTS PASSWORD(options) match, this message does not appear when the two nodes connect with each other.

When the SETROPTS PASSWORD(option) is a RULEx, evaluate the SETROPTS password rule that is listed in the message. These SETROPTS password rules must be consistent when you want two RACF nodes to communicate with each other. You should use the SETROPTS command to change one or both nodes sothat the SETROPTS password rules are consistent. If you plan to allow RACF to synchronize passwords between these nodes, the existing sets of password rules must be merged into a single set that contains the most restrictive of the original rules. Both nodes should then use this new

set of rules. This prevents acceptable passwords on one node from failing on a more restrictive node. When the SETROPTS options are consistent, this message does not appear when the two nodes TARGET each other.

Routing code
2 and 9

Descriptor code
4

4 Trademarks

IBM®, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.