

IBM Security zSecure

*Documentation updates:  
IBM Multi-Factor Authentication for  
z/OS*

**IBM**



IBM Security zSecure

*Documentation updates:  
IBM Multi-Factor Authentication for  
z/OS*

**IBM**



# Chapter 1. IBM® Security zSecure Admin and Audit for RACF User Reference Manual

This chapter lists the documentation updates for the zSecure™ Admin and Audit for RACF User Reference Manual as a result of the IBM Multi-Factor Authentication for z/OS (MFA) Service Stream Enhancement (SSE):

- Chapter 2. RACF Administration Guide, section “User profile tabular display”
- Chapter 2. RACF Administration Guide, section “User profile detail display”
- Chapter 2. RACF Administration Guide, section “Additional selection - Other fields”
- Chapter 3. RACF Audit Guide, section “SETROPTS - RACF settings report”
- Chapter 7. SMF and HTTP Reporting (Events menu), section “Advanced selection criteria: User actions”
- Chapter 10. RACF Access Monitor, section “Specify selection criteria”

## RACF Administration Guide: User profile tabular display

The following panels and the column descriptions are changed:

- “User profile display”
- “User profile display (second screen)”

```

zSecure Admin USER overview                               Line 1 of 4
Command ==>                                              Scroll==> CSR
Users like C##QA0*                                       5 Sep 2000 14:18
  User   Complex  Name                DfltGrp  Owner   RIRP SOAR gC CX MF
  ---   ---      ---                ---      ---    ---  ---  --- ---
  C##QA001 DINO   QA SUBJECT 001      C##QA    C##QA   _____ g  X M
  C##QA002 DINO   QA SUBJECT DUAL AUTH C##QA    C##QA   _____ g  X
  C##QA003 DINO   QA SUBJECT 003      C##QA    C##QA   _____ X MF
  C##QA004 DINO   QA SUBJECT 004      C##QA    C##QA   RI_____ X M
***** BOTTOM OF DATA *****
  
```

Figure 1. User profile display

Table 1. User profile tabular display - Column descriptions

Column name	Description
User	RACF® user profile name (user ID).
Complex	Name for the RACF security database containing this profile.
Name	Programmer name field of RACF profile. Users can change their own programmer name field.
DfltGrp	Default group for the user. Users can change their own default group. The user can only change the default group to a group that is already connected.
Owner	The owning user or group for the user profile.
RIRP	Indicates the user status: <b>R</b> revoked. <b>I</b> due to be revoked through inactivity, <b>R</b> restricted, which means that access through the UACC, global, and ID(*) are not honored. <b>P</b> protected, which means that user ID cannot be used to logon.

Table 1. User profile tabular display - Column descriptions (continued)

Column name	Description
SOAR	Indicates the user attributes: Special, Operations, Auditor, or ROAudit.
gC	The g column indicates that the user is connected to at least one group with the Special, Operations, or Auditor attribute. The C column indicates that the user has at least one class authorization.
CX	C indicates a user certificate. X indicates an expired password.
MF	The M column indicates that effective Multi-Factor Authentication (MFA) information is present for this userid. That is, the userid has an active MFA factor and it is not a PROTECTED userid. The F column indicates that fallback to a password or a passphrase is allowed if the MFA server is unavailable.

```

zSecure Admin USER overview
Command ==>
like C##QA0*
12 Sep 2009 14:18
User Grp LastCon LastUse time LastPwd LastPhrChg PwInt Eff LogD
--- C##QA001 2 09Sep2009 09Sep2009 03:45 04Aug2009 _90 90 SMTW
--- C##QA002 2 10Sep2009 10Sep2009 03:09 04Aug2009 _90 90 SMTW
--- C##QA003 1 29Mar1997 29Mar1997 10:15 29Mar1997 _30 30 SMTW
--- C##QA004 1 13Jun2008 13Jun2008 06:16 24Apr2008 _90 90 SMTW
***** BOTTOM OF DATA *****
Line 1 of 4
Scroll==> CSR

```

Figure 2. User profile display (second screen)

Table 2. User profile tabular display - Column descriptions (scroll right)

Column name	Description
Grp	Number of groups that the user is connected to.
LastCon	Last logon date (with any of the current connect groups).
LastUse	Last logon or update date.
time	Last logon or update time.
LastPwd	Last password change. Empty means never.
LastPhrChg	Last password phrase change. Empty means never.
PwInt	Password interval in days.
Eff	Effective password interval in days. This value combines the PwInt column with the system-wide password interval setting.
LogDays	Days that logon is permitted.

## RACF Administration Guide: User profile detail display

The “User profile display” panel was changed and the descriptions for Multi-Factor Authentication fields were added.

```

zSecure Admin USER overview                               Line 1 of 45
Command ==>>>                                         Scroll==>>> CSR
like C##QA0*                                           1 Mar 2016 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      18Ju196
Inactive, revoked or pending                           No_           Last RACINIT current connects 20Ju100
Days of week user can logon                             SMTWTFS      User's last use date      20Ju100
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                                 12Mar16      Password phrase change date _____
Password expiration date                             11Jun16      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
                                                         _____   Global audit list      ROAUDIT No
                                                         _____   Class authority         _____

Safeguards
Ignore UACC/Glob/* RESTRICTED No_
Log all user actions UAUDIT No_

MFA factor name   Act MFAactive
FACT01#MVB       Yes 24Mar2016
FACT02#MVB       No
MFA Factor       Tag           Tag value
FACT01#MVB       TAG01MVB      Tag01
FACT01#MVB       TAG02MVB      Tag value tag02
FACT02#MVB       TAG02MVB      Tag value tag02

Linked node.user Type   Stat Pwd   Defined (GMT)   Approved (GMT)   Creator
DINO.C##QAWT   Peer   Sync   _____   1998/09/10 11:09 1998/09/10 11:26 C##QA001
Digital certificate labels   Digital certificate names
Primary_____             6F.Jones@Zsecur.NL.CN=Root.OU=CryptoLab.0=Co
Certificate filter label

Identity mapping label   Identity mapping filter
_myFirstRACMAP          UID=armeBert,OU=Tools Development

```

Figure 3. User profile detail display panel

```

zSecure Admin USER overview                               Line 1 of 45
Command ==>                                             Scroll==> CSR
like C##QA0*                                           1 Mar 2016 14:18

  UshrNm  Flg  UshrData
  _ 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##QAIG at 2
  _ Queued command (R): USER C##QA001 SCHEDULE HELPDESK ENABLE (01Mar2002:02Mar20
  _ Inactive commands
  _ Queued command (E): USER C##QA001 SCHEDULE HELPDESK DISABLE (30Aug2000:31Aug2
  _ Commands that have been executed
  _ Queued command (CA): USER C##QA001 SCHEDULE QA#UIT DISABLE (02Sep2000); requ
  _ Other CKGRACF data
  _ Default password set by C##BLU1 at 5 Nov 1998 09:37
  ***** BOTTOM OF DATA *****

```

Figure 4. User profile detail display panel (continued)

**Multi-Factor Authentication fields**

Field	Description
<b>Any effective MFA factor</b>	This shows whether effective Multi-Factor Authentication (MFA) information is present for this userid. That is, the userid has an active MFA factor and it is not a PROTECTED userid.
<b>Fallback to pwd if MFA down</b>	This shows whether the user can logon with a password or passphrase if the MFA server is not available.
<b>MFA factor name</b>	This lists the MFA factors that are present in the USER profile.
<b>Act MFAactive</b>	This shows whether MFA factors are active and when they were activated.
<b>MFA Factor Tag Tag value</b>	This repeated combination field lists the MFA factors in the USER profile with their tags and the associated tag values, if any.



## RACF Administration Guide: Additional selection - Other fields

The Advanced user selection panel and Advanced user selection criteria table were changed.

Menu	Options	Info	Commands	Setup
-----				
zSecure Suite - RACF - User Selection				
<b>Command</b> ==>				
<b>Users like C##QA0*</b>				
Specify additional selection criteria:				
<b>Selection by date</b>				
Last logon/connect.	__	_____		(operator: < <= > >= = <> != )
Last logon/update .	__	_____		(date: yyyy-mm-dd, ddMMyyyy
Password changed .	__	_____		NEVER, DUMPDATE, DUMPDATE-nnn,
Pass phrase changed	__	_____		DUMPDATE-INACTIVE, TODAY,
Creation date . . .	__	_____		TODAY-nnn, TODAY-INACTIVE)
Revoke date . . . .	__	_____		
<b>Logdays selection</b>				
_ Sun	_ Mon	_ Tue	_ Wed	_ Thu
				_ Fri
				_ Sat
<b>Miscellaneous fields</b>				
Password interval .	__	_____		(operator+number or Y/N) / Effective only
Schedule name . . .	__	_____		(schedule name or filter)
Complex . . . . .	__	_____		(complex name or filter)
MFA factor name . .	__	_____		(factor name or filter)

Figure 5. Advanced user selection

Table 3. Advanced user selection criteria

Selection Criteria	Description
<b>MFA factor name</b>	This option allows selection on the name of a factor that is used in an MFA-enabled configuration (MFA: Multi-Factor Authentication). The use of a filter is allowed. Filters can include the following wildcards: % (one character), * (one or more characters), or : (search).

## RACF Audit Guide: SETROPTS - RACF settings report

The “RACF system, ICHSECOP, and general SETROPTS settings” panel was changed.

```

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

  Complex System Collect timestamp
  DINO      DINO      23 Mar 2005 00:07

General RACF properties
Access Control active Yes
Force storage below 16M No
Check all connects GRPLIST Yes
Check genericowner for create Yes
NOADDCREATOR is active Yes
Dynamic CDT active No
RACF local node DINO
RRSF propagate RACF commands No
RRSF propagate applications 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

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

DASD data set protection
Volume level permits DASDVOL No
Erase-on-scratch All

Terminal protection
Terminal protection active Yes
Undefined terminal TERMUACC NONE

TAPE data set protection
Tape dataset check TAPEDSN No
Tape volume protection active Yes
Protection duration RETPD 00000

Program protection
Program control WHEN(PROGRAM) Yes
Program control mode Basic

Auditing options
Audit SPECIAL users Yes
Audit OPERATIONS users Yes
Audit USER profile changes Yes
Audit GROUP profile changes Yes
Audit SECLABELed resources No
Audit command violations Yes
Audit from security level None
Real datasetnames in SMF No
Dataset logoptions Profile
APPLAUDIT is active No

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

Identification/Authentication options
Remember dates INITSTATS Yes
Prevent logon if unused days 255
Revoke after password attempt 5
Old passwords forbidden 32
Password change wait days No
Password change interval 90
Password change warning day 10
Mixed case passwords allowed No
Special passwrld chars allowed No
RACF password algorithm LEGACY
Key change required day 30
MFA support available Yes

Job Entry Subsystem options
Batch userid req BATCHALLRACF Yes
Monitor userid req XBMALLRACF No
Call router exit EARLYVERIFY No
Default uid remote NJEUSERID ????????
Default uid local UNDEFINEDU ++++++
JOBCLASS/SUBMITTER access ct1 No
JOBCLASS/OWNER access ct1 Yes

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

```

Figure 6. RACF system, ICHSECOP, and general SETROPTS settings

```

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

      Complex System   Collect timestamp
      DINO      DINO      23 Mar 2005 00:07

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

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

```

Figure 7. RACF system, ICHSECOP, and general SETROPTS settings (continued)

## SMF and HTTP Reporting (Events menu): Advanced selection criteria: User actions

The “Events - User Action Selection” panel and field explanations were changed.

```

Menu  Options  Info  Commands  Setup
-----
                                zSecure Suite - Events - User Action Selection
Command ==>>> _____
SMF records for all users
Show user related information

Logon/logoff/job start/job end/authentication
_ Password  _ Passphrase  _ MFA  _ Passticket  _ Unknown  _ Failed

Other user activity
_ Revoke/resume activity
_ RACF/CKGRACF commands issued
  _ Successful  _ Failed
  _ Select command type(s)
  _ Include SETROPTS REFRESH/LIST commands
  _ Include ALTUSER RESUME commands
  _ Include CKGRACF commands
_ Affected by RACF/CKGRACF commands

```

Figure 8. Events - User Action Selection panel

Select at least one authentication method to see records for successful authentication events using the selected method. **Unknown** includes job start/job end. Selecting **Failed** will list all failed authentication events.

## RACF Access Monitor: Specify selection criteria

The “Further selection criteria for ID Verify reports” panel was changed.

**zSecure Suite - Access - Further selection**

Command ==>

All access monitor records

**Specify further selection criteria:**

Application name . . . \_\_\_\_\_ (application name or EGN mask)  
Jobname . . . . . \_\_\_\_\_ (jobname or EGN mask)  
Port Of Entry class . . \_\_\_\_\_ (class or EGN mask)  
Port Of Entry . . . . . \_\_\_\_\_ (POE or EGN mask)

**Select authentication method**

- Started
- Password
- Passphrase
- Passticket
- None
- MultiFactor
- Omitted

**Other flags (Y/N/blank)**

- Priv/Trust assigned
- Password changed
- Passphrase changed
- Passticket replay
- Undefined user
- Group-only verify

**User attributes (Y/N/blank)**

- User has special attribute
- User has operations attribute

---

## Chapter 2. IBM Security zSecure CARLa Command Reference

This chapter lists the documentation updates for Chapter 2. SELECT/LIST Fields in the *zSecure CARLa Command Reference* as a result of the IBM Multi-Factor Authentication for z/OS (MFA) Service Stream Enhancement (SSE):

- ACCESS: Access Monitor records
- RACF: RACF profiles
- SMF: SMF records
- SYSTEM: System-wide options

---

### ACCESS: Access Monitor records

The REQ\_VERIFY\_METHOD field description was changed:

#### REQ\_VERIFY\_METHOD

This field shows what method was used to authenticate the user. Possible values for this field are: Omitted, None, Password, Passphrase, Passticket, Started, and MultiFactor. For many verify events, the identity of an existing user is propagated to a new environment. Examples are batch jobs and commands issued through SDSF. In those situations, the REQ\_VERIFY\_METHOD field shows the value None. The width of the field is 12 characters.

---

### RACF: RACF profiles

The following field descriptions were added:

#### ANY\_MFA\_EFFECTIVE

Variable defined in C2RXDEF1 that is true for a userid that can use at least one Multi-Factor Authentication factor. That is to say, an active factor is available and the userid is not PROTECTED. By default, this value is shown as M when true and blank otherwise.

#### FACACDT

This field is found in USER profiles. It contains information about the date when the associated factor for Multi-Factor Authentication was made active. The preferred interface to this database field is the FACTOR\_DATE field.

#### FACTAGS

This field is found in USER profiles. It shows a combination of data pertaining to Multi-Factor Authentication: all tags associated with a factor, and the values of those tags. The preferred interface to this database field is the MFA\_FACTOR\_TAG\_VALUE combination field.

#### FACTOR

This field is found in USER profiles. It lists the factors that are defined for this user for use in Multi-Factor Authentication. The preferred interface to this database field is the FACTOR\_NAME field, because that field also takes into account whether MFA applies to the userid.

#### FACTOR\_ACTIVE

This flag field is found in USER profiles. It indicates whether the associated factor for Multi-Factor Authentication is active.

**FACTOR\_DATE**

This field is found in USER profiles. It shows the date when the associated factor for Multi-Factor Authentication was made active. It blanks or remains blank if the factor is not active.

**FACTOR\_NAME**

This field is found in USER profiles. It lists the factors that are to be used for this user in Multi-Factor Authentication.

**FACTORN**

This field is found in USER profiles. It represents the number of factors defined for this user for use in Multi-Factor Authentication.

**MFA\_FACTOR\_TAG\_VALUE**

This field is found in USER profiles. It shows a combination of data pertaining to Multi-Factor Authentication: the name of the factor, the name of a tag associated with that factor, and the value of that tag.

**MFA\_FALLBACK**

This flag field is found in USER profiles. It indicates whether the user is allowed to authenticate using only a password or password phrase when trying to enter the system at a moment when the Multi-Factor Authentication server cannot be reached.

**MFA\_TAG\_FACTOR**

This field is found in USER profiles. It lists the factors that are defined for this user for use in Multi-Factor Authentication. This field is intended for SELECT/EXCLUDE processing. Otherwise, the preferred interface to this field is the MFA\_FACTOR\_TAG\_VALUE combination field.

**MFA\_TAG\_NAME**

This field is found in USER profiles. It lists the tags associated with the factors that are defined for this user for use in Multi-Factor Authentication. This field is intended for SELECT/EXCLUDE processing. Otherwise, the preferred interface to this field is the MFA\_FACTOR\_TAG\_VALUE combination field.

**MFA\_TAG\_VALUE**

This field is found in USER profiles. It lists the tag values associated with the factors that are defined for this user for use in Multi-Factor Authentication. This field is intended for SELECT/EXCLUDE processing. Otherwise, the preferred interface to this field is the MFA\_FACTOR\_TAG\_VALUE combination field.

**MFAFLBK**

This field is found in USER profiles. It contains information about whether the user is allowed to authenticate using only a password or password phrase when trying to enter the system at a moment when the Multi-Factor Authentication server cannot be reached. The preferred interface to this database field is the MFA\_FALLBACK field.

**MFDATA**

This field is found in GENERAL profiles in the MFADEF class and is part of the MFA segment. It contains the data that the MFA server has put there.

**NOMFA**

This field can only be used for SELECT/EXCLUDE processing. It selects non-MFA segments.

---

## SMF: SMF records

This section lists the documentation updates for NEWLIST TYPE=SMF.

## Field descriptions

The following field descriptions are changed or added:

### **AUTHENTICATOR\_USED**

This field describes the authenticator that was used for a successful authentication. It is only found in RACF processing and R\_auditx records (SMF record types 80 and 83) pertaining to a RACINIT event (subtype 1) with an event qualifier 40 (Successful multi-factor authentication).

Although technically a repeated field, it is expected to show a single authenticator at most.

The AUTHENTICATOR\_USED field can have the following values:

*Table 4. SMF record AUTHENTICATOR\_USED field values*

Value	Description
Password	Password Successful
Passphrase	Password Phrase Successful
Passticket	Passticket Successful
MultiFactor	Multi-factor authentication Successful

### **COMPCODE, COMPLETION\_CODE**

This field describes a job or step completion code. It is available in some SMF type 80 and 83 records as well as in SMF record types 4, 5, and 30. It can describe a return code (on successful completion), one or two reason codes, a system abend code possibly followed by an abend reason code, or a user abend code.

When a COMPCODE field value does not fit in a column, asterisks are shown instead of truncated decimal or hexadecimal codes. COMPCODE selections still pertain to the original field value, which should not contain any asterisks.

The COMPCODE field can have the following layouts:

*Table 5. MF record COMPCODE field - values for output processing*

Value	Description
RC $n$	Reason code or job/step completion code (decimal)
RC $m-n$	Reason codes (decimal)
Sccc	System ABEND code (hexadecimal)
Sccc-cc	System ABEND code and reason code (hexadecimal)
Ucccc	User ABEND code (decimal)

### **EVENT**

The following rows were added to the Event 1: Qualifier codes and descriptions table:

*Table 6. Event 1: Qualifier codes and descriptions*

Qualifier	Meaning
39	No RACF user id found for distributed identity
40	Successful Multi-Factor Authentication

Table 6. Event 1: Qualifier codes and descriptions (continued)

Qualifier	Meaning
41	Failed Multi-Factor Authentication
42	Multi-Factor Authentication unavailable
43	Multi-Factor Authentication partially succeeded

### RACF\_AUTH\_INFO

This field describes the Multi-Factor Authentication information flags found in some SMF type 80 and 83 records pertaining to RACINIT events.

Because many flags can be set at the same time, the default output of this bitfield is in a condensed format; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 30; for example, RACF\_AUTH\_INFO(EXPLODE,30). The following table lists sample RACF\_AUTH\_INFO bitmask values that can be used for SELECT/EXCLUDE processing, the condensed output, the exploded output, and the meaning.

Table 7. RACF\_AUTH\_INFO values

Select/Exclude	Condensed	Exploded	Meaning
'1.....'	V.....	Authenticated from VLF	Authenticated from VLF
'.1.....'	.A.....	User has active MFA factor	User has active MFA factor(s)
'..1.....'	..F....	MFA fallback allowed	MFA user allowed to fall back when no MFA decision can be made
'...1....'	...N...	No MFA decision	No MFA decision for MFA user
'....1...'	....X..	MFA requests pw-expired RC	MFA requested that RACROUTE REQUEST=VERIFY return the password-expired return code
'.....1.'	.....I.	MFA requests new-pw-invalid RC	MFA requested that RACROUTE REQUEST=VERIFY return the new-password-invalid return code
'.....1.'	.....P	MFA partially successful	MFA only partially succeeded

### RACF\_AUTH\_USED

This field describes the Multi-Factor Authentication flags that show which authenticators were used. The flags are found in some SMF type 80 and 83 records pertaining to RACINIT events.

Because many flags can be set at the same time, the default output of this bitfield is in a condensed format; full output split into several lines can be requested using the EXPLODE output modifier and an overriding length of 21, RACF\_AUTH\_USED(EXPLODE,21) for example. The following table lists sample RACF\_AUTH\_USED bitmask values that can be used for SELECT/EXCLUDE processing, the condensed output, the exploded output, and the meaning.



Table 8. RACF\_AUTH\_USED values

Select/Exclude	Condensed	Exploded	Meaning
'1.....'	E.....	Password evaluated	Password evaluated
'.1.....'	.S.....	Password successful	Password authentication successful
'..1.....'	..E.....	Phrase evaluated	Password phrase evaluated
'...1....'	...S....	Phrase successful	Password phrase authentication successful
'....1...'	....E...	Passticket evaluated	Passticket evaluated
'.....1.'	.....S..	Passticket successful	Passticket authentication successful
'.....1.'	.....S.	MFA successful	Multi-factor authentication successful
'.....1'	.....U	MFA unsuccessful	Multi-factor authentication unsuccessful

## Fields found in RACF processing records

The following rows are changed or added to the SMF RACF processing records - field descriptions table:

Table 9. SMF RACF processing records - field descriptions

Field name	Meaning	Event types
AUTHENTICATOR_USED	Authenticator used in successful authentication	RACINIT
COMPCODE	Job or step completion code	RACINIT
RACF_AUTH_INFO	MFA authentication information	RACINIT
RACF_AUTH_USED	Authentication method used	RACINIT

---

## SYSTEM: System-wide options

The MFA\_AVAILABLE field description was added:

### MFA\_AVAILABLE

This flag field indicates whether or not Multi-Factor Authentication support is available. For ACF2 and Top Secret systems, this flag field returns missing.



---

## Chapter 3. IBM Security zSecure Command Verifier User Guide

This chapter lists the documentation updates for the *zSecure Command Verifier User Guide* as a result of the IBM Multi-Factor Authentication for z/OS (MFA) Service Stream Enhancement (SSE):

- Chapter 4. Auditing commands and policy effects:
  - “Structure of =CMDAUD policy profile”
  - “Format of the Command Audit Trail data display”
- Chapter 5. Policy profiles:
  - “Controlled temporary system-level attributes”
  - New: ““Profiles to manage Multi-Factor Authentication (MFA) data” on page 16”
  - “Profiles that manage non-base segments”: title was changed to “Profiles for controlling management of non-base segments”
  - “Scoping rules to manage segments”
  - New: ““USER MFA data management functions” on page 18”

---

### Structure of =CMDAUD policy profile

For *data-type*, the description for value =SEGMENT was changed.

#### =SEGMENT

Information about adding, changing, and deleting segments.

Although technically, the MFA data in the USER profile is not kept in a separate segment, modifications to the MFA data are recorded based on the =SEGMENT policy for the Command Audit Trail.

---

### Format of the Command Audit Trail data display

The description of the Segments section was changed.

- **The Segments section**

**The Segments section** contains the information about the last change to non-base segments. The first line starts with the word *Segment:*, followed by an abbreviated name for the segment. The remainder of the line contains information about the type of change, like add, change, delete, when the change was made, and which user ran the command. It also contains the highest non-zero return code from the pre-, RACF, and post-command. For modifications to existing segments, only the last change is shown.

Collection is controlled by the policy profile

```
C4R.class=CMDAUD.=SEGMENT.profile-identification
```

A separate block (add, change, delete) is shown for each segment that was modified. The following segments and pseudo-segment are currently supported.

**USER** CICS®, DFP, LANGUAGE, NETVIEW, OMVS, OPERPARM, TSO, WORKATTR, OVM, DCE, NDS, LNOTES, KERB, PROXY, EIM, CSDDATA, MFA

**GROUP**

DFP, OMVS, OVM, TME, CSDDATA

## DATASET

DFP, TME

## General Resource

SESSION, DLFDATA, SSIGNON, STDATA, SVFMR, TME, KERB, PROXY, EIM, CDTINFO, ICTX, CFDEF, ICSF, SIGVER, MFA

---

## Controlled temporary system-level attributes

A policy profile was added to the the figure with policy profiles used to determine whether Controlled Temporary system-level attributes can be assigned:  
C4R.USER.MFA.

---

## Profiles to manage Multi-Factor Authentication (MFA) data

RACF implemented support for Multi-Factor Authentication through new function APARs OA48359 and OA48650. The required data can be added to USER profiles and to general resource profiles in the MFADEF resource class.

In the USER profiles, the relevant data is kept in several MFA-related fields in the BASE segment. In the MFADEF resource class, the data is kept in the MFA segment. Although technically, the MFA data in the USER profile is not kept in a separate segment, zSecure Command Verifier handles the information as if an independent segment is being used. That means that policy profiles and the existing policy profiles for existing segments are used similarly. The following policy profiles are used to control management of MFA data in the USER profile:

Table 10. Policy profiles to control management of MFA data in the USER profile

Keyword	Value	Profile
(NO)MFA	n/a	C4R.USER.MFA
		C4R.USER.MFA.=RACUID
		C4R.USER.MFA./SCOPE
(NO)PWFALLBACK	n/a	C4R.USER.MFA.PWFALLBACK.owner.userid
(DEL)FACTOR	<i>factor-name</i>	C4R.USER.MFA.FACTOR.ID. <i>factor-name</i> .owner.userid
(NO)ACTIVE	<i>factor-name</i>	C4R.USER.MFA.FACTOR.ACTIVE. <i>factor-name</i>
TAG	<i>factor-name</i> <i>tag-name</i>	C4R.USER.MFA.FACTOR.TAG. <i>factor-name</i> . <i>tag-name</i>
DELTAG	<i>factor-name</i> <i>tag-name</i>	C4R.USER.MFA.FACTOR.TAG. <i>factor-name</i> . <i>tag-name</i>
NOTAGS	n/a	C4R.USER.MFA.FACTOR.TAG. <i>factor-name</i> .+

For more information about these profiles, see Profiles for controlling management of non-base segments and “USER MFA data management functions” on page 18.

The MFA information for the profiles in the MFADEF general resource class is kept in the MFA segment. The contents of this MFA segment cannot be controlled using RACF commands. The only function that is provided is adding or removing the MFA segment in these profiles. The following policy profiles are used to control management of the MFA segment of profiles in the MFADEF general resource class:

Table 11. Policy profiles used to control management of MFA segment of profiles in MFADEF general resource class

Keyword	Value	Profile
(NO)MFA	n/a	C4R.MFADEF.MFA
		C4R.MFADEF.MFA./SCOPE

For more information about these profiles, see Profiles for controlling management of non-base segments.

---

## Profiles for controlling management of non-base segments

The introduction of this section was changed:

RACF allows management of information in non-base segments, such as, the OMVS and TSO segments to all System-SPECIAL users and to all users with sufficient access to profiles in the FIELD class. The latter method is often referred to by the term *Field Level Access Checking*. In some situations, it might be desirable to restrict management of these types of segments even further. Although MFA data in the USER profile is technically not in a separate segment, zSecure Command Verifier handles the information as if it is contained in a segment. In the remainder of this section, the variable segment also applies to the MFA data in the USER profile. To allow control over the non-base segment, zSecure Command Verifier implements three types of profiles.

The values that are supported for the qualifier segment in the preceding profiles were changed:

**USER** CICS, DFP, LANGUAGE, NETVIEV, OMVS, OPERPARM, TSO, WORKATTR, OVM, DCE, NDS, LNOTES, KERB, PROXY, EIM, CSDATA, MFA

**GROUP**  
DFP, OMVS, OVM, TME, CSDATA

**DATASET**  
DFP, TME

**General Resource**  
SESSION, DLFDATA, SSIGNON, STDATA, SVFMR, TME, KERB, PROXY, EIM, CDTINFO, ICTX, CFDEF, ICSF, SIGVER, MFA

---

## Scoping rules to manage segments

The following information was added:

Although technically, the MFA data in the USER profile is not kept in a separate segment, zSecure Command Verifier handles the MFA data in the USER profile as if it is contained in a segment. The /SCOPE policy profiles as described in this section can be used to limit management of MFA data in USER profiles to users with group-SPECIAL or system-SPECIAL. Access to profiles in the FIELD class is not required.

## USER MFA data management functions

RACF implemented support for Multi-Factor Authentication through new function APARs OA48359 and OA48650. Part of the required data must be added to USER profiles.

In the USER profiles, the relevant data is kept in several MFA-related fields in the BASE segment. The following policy profiles are used to control management of MFA-specific fields in the USER profile:

Table 12. Policy profiles to control management of MFA-specific fields in the USER profile

Keyword	Value	Profile
(NO)PWFALLBACK	n/a	C4R.USER.MFA.PWFALLBACK. <i>owner.userid</i>
(DEL)FACTOR	<i>factor-name</i>	C4R.USER.MFA.FACTOR.ID. <i>factor-name.owner.userid</i>
(NO)ACTIVE	<i>factor-name</i>	C4R.USER.MFA.FACTOR.ACTIVE. <i>factor-name</i>
TAG	<i>factor-name</i> <i>tag-name</i>	C4R.USER.MFA.FACTOR.TAG. <i>factor-name.tag-name</i>
DELTAG	<i>factor-name</i> <i>tag-name</i>	C4R.USER.MFA.FACTOR.TAG. <i>factor-name.tag-name</i>
NOTAGS	n/a	C4R.USER.MFA.FACTOR.TAG. <i>factor-name.+</i>

The profiles in the preceding table describe the policies that can be used to verify the keywords and values as entered by the terminal user. The following list shows detail information about these policies and the supported access levels.

- **C4R.USER.MFA.PWFALLBACK.*owner.userid***

This profile describes the authorization to set the PWFALLBACK attribute for the user. The PWFALLBACK attribute is used during logon if the MFA server is not available or is unable to determine the validity of an active factor. The following access levels are used:

**No profile found**

This control is not implemented. Only RACF authorization is used to control setting the PWFALLBACK or NOPWFALLBACK attribute.

**NONE**

The terminal user is not authorized to assign either PWFALLBACK or NOPWFALLBACK. The command is failed.

**READ** The terminal user is authorized to assign NOPWFALLBACK. This is the default value on the ALTUSER command

**UPDATE**

The terminal user is authorized to assign PWFALLBACK and NOPWFALLBACK.

**CONTROL**

Same as UPDATE.

- **C4R.USER.MFA.FACTOR.ID.*factor-name.owner.userid***

This profile describes the authorization to add an MFA factor for a user, to modify options for the specified MFA factor, or to remove an MFA factor. The keywords to set the ACTIVE status, or to modify the list of TAGs, apply to the specified factor. The following access levels are used:

**No profile found**

This control is not implemented. Only RACF authorization is used to control adding, modifying, or removing the specified factor *factor-name*.

**NONE**

The terminal user is not authorized to add, modify, or remove the specified factor *factor-name*. The command is failed.

**READ** Same as NONE.

**UPDATE**

The terminal user is authorized to manage the specified factor *factor-name*.

**CONTROL**

Same as UPDATE.

- **C4R.USER.MFA.FACTOR.ACTIVE**,*factor-name*

This profile describes the authorization to activate an MFA factor for a user. This policy profile is used in conjunction with the FACTOR.ID policy profile. The FACTOR.ID policy profile controls the authority to manage the FACTOR for a particular user. The current policy profile controls the use of the ACTIVE status of the factor.

**No profile found**

This control is not implemented. Only RACF authorization is used to control the status of the specified factor.

**NONE**

The terminal user is not authorized to modify the status of the specified factor *factor-name*. The command is failed. The terminal user is also not allowed to explicitly specify the default value of NOACTIVE for the status of the factor.

**READ** Same as NONE.

**UPDATE**

The terminal user is authorized to change the ACTIVE status of the specified factor *factor-name*.

**CONTROL**

Same as UPDATE.

- **C4R.USER.MFA.FACTOR.TAG**,*factor-name.tag-name*

This profile describes the authorization to manage TAGs for the specified factor. This policy profile is used in conjunction with the FACTOR.ID policy profile. The FACTOR.ID policy profile controls the authority to manage the FACTOR for a particular user. The current policy profile controls the management of the TAGs of the factor. If multiple tags are set or removed in a single command, the terminal user must have sufficient authority for all tags. If the terminal user has insufficient authority to one or more tags, the entire command is failed. The special value + (plus sign) is used for the *tag-name* to designate the use of the NOTAGS keyword.

**No profile found**

This control is not implemented. Only RACF authorization is used to control managing TAGS.

**NONE**

The terminal user is not authorized to manage the tag *tag-name* for the factor *factor-name*. The command is failed.

**READ** Same as NONE.

**UPDATE**

The terminal user is authorized to manage the tag *tag-name* for the factor *factor-name*.

**CONTROL**

Same as UPDATE.



---

## Chapter 4. IBM Security zSecure Messages Guide

This chapter lists the documentation updates for the *zSecure Messages Guide* as a result of the IBM Multi-Factor Authentication for z/OS (MFA) Service Stream Enhancement (SSE).

---

**C4R413E**    **Not allowed to set PWFALLBACK for user *userid*, command terminated**

**Explanation:** The terminal user is not authorized to specify PWFALLBACK for the indicated *userid*.

---

**C4R414E**    **Not allowed to set NOPWFALLBACK for user *userid*, command terminated**

**Explanation:** The terminal user is not authorized to specify NOFALLBACK for the indicated *userid*.

---

**C4R415E**    **Not allowed to manage factor *factor-name* for user *userid*, command terminated**

**Explanation:** The terminal user is not authorized to add, change, or remove factor *factor-name* for the indicated *userid*.

---

**C4R416E**    **Not allowed to change active status of factor *factor-name*, command terminated**

**Explanation:** The terminal user is not authorized to change the active or inactive status of factor *factor-name*.

---

**C4R417E**    **Not allowed to change tag *tag-name* of factor *factor-name*, command terminated**

**Explanation:** The terminal user is not authorized to change the tag value for tag *tag-name* of factor *factor-name*.

---

**C4R418E**    **Not allowed to remove tag *tag-name* of factor *factor-name*, command terminated**

**Explanation:** The terminal user is not authorized to remove the tag *tag-name* for factor *factor-name*.

---

**C4R419E**    **Not allowed to remove all tags of factor *factor-name*, command terminated**

**Explanation:** The terminal user is not authorized to remove all tags for factor *factor-name*.







Printed in USA