z/OS
2.5

RACF Support for IBM Multi-Factor Authentication for z/OS (IBM MFA)

Note

Before using this information and the product it supports, read the information in “Notices” on page 51.

This edition applies to Version 2 Release 5 of z/OS® (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2023-06-28

Contents

Figures

Tables

Abstract for RACF Support for IBM Z Multi-Factor Authentication (IBM MFA)

Purpose of this information This information is a collection of all of the information that you need to understand and exploit the IBM Multi-Factor Authentication for z/OS (IBM MFA). Some of the information also exists elsewhere in the z/OS library.

Who should read this information This information is intended for system programmers who are using IBM Multi-Factor Authentication for z/OS (IBM MFA).

Related information

To find the complete z/OS library, go to IBM Documentation (www.ibm.com/docs/en/zos).

How to send your comments to IBM

We invite you to submit comments about the z/OS product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead “If you have a technical problem” on page xi.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM® Documentation function
If your comment or question is about the IBM Documentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdocs@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The section title of the specific information to which your comment relates
- The comprehensive content collection title: RACF Support for IBM Multi-Factor Authenication for z/OS (IBM MFA)
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Chapter 1. What is RACF support for IBM Multi-Factor Authentication (IBM MFA)

Today, the most common way for users to access z/OS systems is by the use of passwords or password phrases. Due to the simplicity of passwords, they can present a relatively simple point of attack for exploitation. In order for systems that rely on passwords to be secure, they must enforce password controls and provide user education. Some of the common problems with a simple password are that users tend to: choose common passwords, write down their passwords, or unintentionally install malware that can key log passwords.

A more secure option is for systems to require multiple authentication factors to verify the user's identity.

A multi-factor authentication system requires that multiple authentication factors be presented during logon to verify a user's identity. Each authentication factor must be from a separate category of credential types:

- Something you know: A password or security question
- Something you have: An ID badge or cryptographic token device
- Something you are: Fingerprint or other biometric data

By requiring multiple authentication factors, a user's account can not be compromised if one of their factors is discovered.

IBM MFA on z/OS

IBM Multi-Factor Authentication for z/OS, RACF® provides support for authenticating with multiple authentication factors. RACF users can be configured to require authentication through IBM MFA. For these select users, RACF calls IBM MFA to help in making the authentication decision during logon processing.

IBM MFA infrastructure

RACF is enhanced to provide infrastructure to enable IBM Multi-Factor Authentication for z/OS to integrate directly with the security server. The RACF MFA infrastructure consists of updates to the database, commands, callable services, logon processing and utilities.

Chapter 2. Getting started with RACF support for IBM MFA

While the MFA support for RACF can be implemented on a per user basis, consider taking the following actions before making changes.

1. Learn about IBM Multi-Factor Authentication for z/OS.
2. Create a backup copy of your RACF database.
3. Apply the RACF MFA APARs to all systems sharing the RACF database.
4. Configuring RACF for IBM MFA.

Learn about IBM Z Multi-Factor Authentication

For more information about IBM Multi-Factor Authentication for z/OS, see *IBM Z Multi-Factor Authentication User's Guide* and *IBM Z Multi-Factor Authentication Installation and Customization*.

Create a backup of your RACF database

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

There are two utilities you can use to create a backup database:

- IRRUT200 serializes on the RACF database and creates an exact, block-by-block copy of it.

  This exact copy can help performance when you are maintaining statistics on your backup database. IRRUT200 can be used only if you are creating a backup database that is the same size and on the same device type as the input database. If you specify PARM=ACTIVATE in your JCL, IRRUT200 activates the backup copy without allowing the RACF database to be updated between the copy and activate operations, keeping the backup and primary data sets synchronized.

- IRRUT400 creates a copy of your database and can be used to change its size.

  IRRUT400 also reorganizes the contents of the output RACF database. Use this utility if you are copying between different device types. You can also use IRRUT400 to extend the RACF database before it becomes full.

It is important to use the RACF-provided utilities when copying an active RACF database, because they serialize to protect the data in your database. If, however, your database is inactive, you can use other block copy utilities, such as IDCAMS REPRO.

Options for updating backup databases

The RACF data set name table specifies the data set names for both the primary and backup RACF databases, and the recovery option. If the primary database is split, you specify several pairs of entries. If you elect to use the RACF data set name table, you can choose from three backup options:

1. **All updates duplicated on the backup database**

   When you update the primary database, the backup database is also updated. If you choose this option, your backup database must be a copy of the primary database that existed at RACF initialization. Switching to this backup database is transparent to the users.

   The cost, in terms of RACF processing for this option, is high if you use many discrete profiles and do not use SETROPTS RACLIST processing.

2. **All updates, except for statistics, duplicated on the backup database**

This option is similar to the first option, except that changes you make to the primary database for the sole purpose of updating statistics are not made on the corresponding backup database. If you are maintaining statistics on the primary database and you must switch to the backup database, you might lose some statistics.

Note: However, if SETROPTS INITSTATS is on, a limited subset of statistics is maintained on the backup.

The cost, in terms of RACF processing for this option, can be appreciable if a high proportion of your activity is changing RACF profiles. However, the overhead is less than for the first option, and your backup database is current in the event of an error on your primary.

Guideline: Use this option in your data set name table.

3. **No updates duplicated on the backup database**

   With this option, your backup database is allocated but inactive. When you make changes to the primary database, the corresponding backup database is not updated. If you switch to this backup database when there is a failure in your primary database, you bring a down-level RACF database into operation.

   Note: If you activate the backup database, RACF will start recording the updates on the backup.

   The cost, in terms of RACF processing for this option, is negligible, but system operation and recovery could be difficult, depending on how out-of-date the information in the database is.

Apply the RACF MFA 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.

- OA48359
- OA48650
- OA50016
- OA50930
- OA50931
- OA53002
- OA53013
- OA54920

RACF exit considerations

Similar to a PassTicket behavior, a RACROUTE REQUEST=VERIFY pre-processing exit will not have any indication that the contents of the password fields are actually password data or data for IBM Multi-Factor Authentication for z/OS. The VERIFY post-processing exit will be able to determin if the user successfully authenticated with z/OS MFA by checking the new ACEEMFAA bit.

RACF performance considerations

Authentication requests using MFA may be slower than non MFA authentication requests. At the very least, MFA authentication will incur extra path length when calling IBM Multi-Factor Authentication for z/OS. Depending on the factor type, there may be additional considerations such as network calls to external authentication servers. Non MFA authentication requests should have little to no noticeable performance degradation.

Chapter 3. Configuring RACF for IBM MFA

There are a number of steps to be completed in order to begin using IBM Multi-Factor Authentication for z/OS with RACF. IBM MFA should be installed as described in *IBM Z Multi-Function Authentication Installation and Customization*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website. Then, perform the following steps to configure RACF for MFA:

1. Define the factor to RACF:

   An IBM MFA factor is defined by creating an MFADEF class profile with the name FACTOR.*factor-name*. Supported authentication factors are listed in the IBM Multi-Factor Authentication for for z/OS product documentation. Note that a single factor name may enforce multiple authentication factors during logon.

   For example, to define the RSA SecurID factor supported by IBM MFA:

   ```
   RDEFINE MFADEF FACTOR.AZFSIDP1
   ```

2. Assign the factor to users:

   MFA factor data can be added to a RACF user ID with the MFA keyword of the ALTUSER command. The factor must be defined in the MFADEF class before this step can be completed. The sub-keywords of MFA are:

   FACTOR/DELFACTOR
   Use the FACTOR keyword to identify the name of the factor that is being added or modified.

   Use the DELFACTOR keyword to delete a factor from a user profile.

   ACTIVE/NOACTIVE
   Use the ACTIVE keyword to activate a factor for use during logon.

   Use the NOACTIVE keyword to disable a factor and revert to password checking.

   TAGS/DELTAGS/NOTAGS
   Use the TAGS keyword to assign configuration data that is specific to the factor. The data is specified in *name:value* format. The IBM Multi-Factor Authentication for z/OS product documentation contains information on supported tags. IBM MFA is called to validate the data. The MFA started task must be available when assigning tags, or the ALTUSER command fails.

   Use the DELTAGS keyword to delete specific tags.

   Use the NOTAGS keyword to delete all tags for the specified factor.

   PWFALLBACK/NOPWFALLBACK
   Use the PWFALLBACK keyword to allow the user to logon with a RACF password or password phrase whenever the ability to perform multi-factor authentication is not available (for example, the MFA started task is down). PWFALLBACK is not factor-specific.

   Use NOPWFALLBACK to require the user to always authenticate using MFA.

   ADDPOLICY/DELPOLICY
   Use the ADDPOLICY keyword to add the user's list of MFA authentication policies where *policy-name* is the name of the MFA policy profile defined in the MFADEF class.

   Use the DELPOLICY keyword to delete the specified policies from the user's list of MFA policies.

   NOMFA
   Use the NOMFA keyword to remove all MFA data from a user's profile.

   See the *z/OS Security Server RACF Command Language Reference* for more information on the MFA keywords.

   Example:

To require a user to authenticate with RSA SecurID, but allow the user to logon with their RACF password when MFA is unavailable:

```
ALTUSER SLJAXON MFA(FACTOR(AZFSIDP1) ACTIVE PWFALLBACK
                  TAGS(SIDUSERID:SamLJ))
```

3. Activate MFA checking:

   When setup is complete, activate the MFADEF class.

   ```
   SETROPTS CLASSACT(MFADEF)
   ```

   When this is completed, RACF will call IBM Multi-Factor Authentication for z/OS to perform user authentication for any user who has an active MFA factor.

   MFA checking can be disabled for all users by deactivating the MDADEF class:

   ```
   SETROPTS NOCLASSACT(MFADEF)
   ```

MFA considerations for the RACF password and password phrase

MFA information cannot be assigned to a PROTECTED user, and thus an MFA user must have a password or password phrase.

When the user is assigned the NOPWFALLBACK attribute, the password/phrase cannot be used to logon. In this case, consider assigning the user a long, random password phrase.

When the user is assigned the PWFALLBACK option, the user needs to maintain the password as usual. However, the password will not be able to be changed during logon unless MFA is unavailable, the user's password is expired, and the application prompts the user to enter a new password. The user's password can be changed using the PASSWORD or ALTUSER command.

MFA application bypass

In some cases it may be desireable to bypass select z/OS applications from MFA processing. IBM MFA provides controls to allow the RACF administrator to name applications for which MFA authentication will not be enforced. The MFA bypass controls allow for different bypass policy for different RACF users.

For more details on the MFA application bypass feature, refer to *IBM Z Multi-Function Authentication Installation and Customization* and *IBM Z Multi-Function Authentication User's Guide* in the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

MFA policy

Installations can create MFA policies to define a set of rules that users must follow when authenticating with IBM MFA. The policy attributes are defined in the MFPOLICY segment of profiles in the MFADEF class. These policies can be associated with individual users with the ALTUSER ADDPOLICY keyword.

For information about on MFA policies, refer to *IBM Z Multi-Function Authentication Installation and Customization* and *IBM Z Multi-Function Authentication User's Guide* in the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

MFA compound In-Band

MFA users may be provisioned so that they are required to authenticate with both a token device code and their RACF authenticator (password or password phrase). Users configured for compound in-band may enter their token code and RACF authenticator concatenated together in the password phrase field of an application with a separator character between the two values. When the RACF authenticator is expired it can be changed by passing the new value into the new password or new password phrase field of the application by itself without the token code portion.

For more information on MFA compound in-band support, refer to *IBM Z Multi-Function Authentication Installation and Customization* and *IBM Z Multi-Function Authentication User's Guide* in the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

Chapter 4. RACF auditor support for IBM MFA

Logging, the recording of data about specific events, is the key to auditing the use of RACF at your installation. You must ensure that RACF logs the information you need. RACF uses the system management facilities (SMF) to log data about various RACF events. RACF writes SMF records to an SMF data set or log stream.

RACF always logs information about certain events because knowing about these events is essential to an effective data-security mechanism. The events that RACF logs for IBM MFA is:

- A successful RACROUTE REQUEST=VERIFY under the following conditions:
  - SETROPTS AUDIT(USER) is active and a user's password or password phrase is changed
  - authentication using a PassTicket
  - authentication of an IBM Multi-Factor Authentication user using a password or password phrase.

Chapter 5. Identifying and verifying RACF IBM MFA users

RACF identifies you when you log on to the operating system that you want to use. It does so by requiring a user identification, the user ID, which is a unique identification string. RACF then verifies that you are the user you say that you are by requesting and checking a password. Each RACF user ID has a unique password. You should be the only one who knows your password. That way, RACF can ensure personal accountability.

You might also be assigned a password phrase. If so, the first time you log on using your password phrase RACF requires you to supply a new password phrase of your choice. Your password phrase might expire after a certain time interval, so you might need to change it periodically.

You can be required to authenticate with multiple authentication factors instead of a password or password phrase. In this case, what you enter when you log on is determined by IBM Multi-Factor Authentication for z/OS. For example, you might be required to enter an RSA SecurID token code and PIN. See *IBM Z® Multi-Function Authentication User's Guide* for more information.

Chapter 6. RACF commands for IBM MFA

This topic includes the RACF commands that are new or have been enhanced to support IBM Multi-Factor Authentication for z/OS (IBM MFA):

- ALTUSER
- RDEFINE
- RALTER
- RLIST
- LISTUSER

ALTUSER

The ALTUSER command is enhanced to support adding multi-factor information to the base segment of a user profile. Any user with an ACTIVE MFA factor will be authenticated through IBM Multi-Factor Authentication for z/OS duruing logon.

Authorization required

If you have the SPECIAL attribute, you can use the MFA operands.

If the owner of the user profile is within the scope of a group in which you have the group- SPECIAL attribute, you can use the MFA operands.

If you are the owner of the user's profile, you can use the MFA operands.

Syntax

```
[ MFA(
        [ PWFALLBACK|NOPWFALLBACK ]
        [ FACTOR(factor-name) | DELFACTOR(factor-name) ]
        [ ACTIVE|NOACTIVE ]
        [ TAGS(tag-name:tag-value ...)
             | DELTAGS(tag-name ...)
             | NOTAGS ]
        [ ADDPOLICY(policy-name ...)
             | DELPOLICY(policy-name ... | *) ]
        )
     | NOMFA ]
```

Parameters

MFA | NOMFA

MFA
Specifies multi-factor authentication information for the user profile being changed. Information is stored in the base segment of the user's profile. MFA can not be specified for a PROTECTED user.

The MFADEF class must be active before a user can logon with IBM MFA.

See *z/OS Security Server RACF Security Administrator's Guide*.

PWFALLBACK|NOPWFALLBACK

PWFALLBACK
When IBM MFA is unavailable or is unable to determine the validity of an ACTIVE factor, this user can logon to the system using any existing RACF authenticators such as their password, password phrase or PassTicket.

NOPWFALLBACK
When IBM MFA is unavailable or is unable to determine the validity of an ACTIVE factor, this user will not be able to logon to the system with any existing RACF authenticators. NOPWFALLBACK is the default.

FACTOR|DELFACTOR

FACTOR(*factor-name*)
Specifies an authentication factor for a user. If the user is not already registered to the factor, the factor will be added to the user. The specified factor must be defined in an MFADEF class profile named FACTOR.<factorName>. Other ALTUSER keywords such as ACTIVE and TAGS are specific to this specified factor.

Factor-name is a 1 - 20 character identifier. The characters can be alphabetic, numeric, or national.

A user is limited to 10 total factors. Only one factor may be specified in a single ALTUSER command.

DELFACTOR(*factor-name*)
Deletes the specified factor from the list of authentication factors registered to this user.

Factor-name is a 1 - 20 character identifier. The characters can be alphabetic, numeric, or national.

ACTIVE|NOACTIVE

ACTIVE
The user is required to authenticate to IBM MFA with the specified factor to logon to the system when the MFADEF class is active.

NOACTIVE
The user is not required to authenticate to IBM MFA with the specified factor to logon to the system. NOACTIVE is the default.

TAGS|DELTAGS|NOTAGS

TAGS(*tag-name:tag-value...*)
Specifies tags and values for the specified factor.

The *tag-name* and *tag-value* pairs are factor specific and are defined by IBM MFA. ALTUSER calls IBM MFA to validate tag-names and tag-values. IBM MFA must be available for RACF to process the TAGS keyword. IBM MFA may reject a *tag-name* or *tag-value* during ALTUSER processing. IBM MFA may utilize these values during logon processing to authenticate a user. Refer to *IBM Z Multi-Function Authentication User's Guide* for documentation of each factor's configuration data parameters.

When the *tag-name* is not already present in the TAGS for the specified factor the *tag-name* is added. When the *tag-name* is already present for the specified factor, it is replaced with the new *tag-value*.

The *tag-name* is a 1 - 20 character case insensitive identifier and can consist of alphabetic or numeric characters. A factor is limited to 20 total tags.

The *tag-value* can be 1 - 1024 characters and can consist of any character. If the *tag-value* you specify contains any blanks, the *tag-name:tag-value* pair must be enclosed in quotation marks.

DELTAGS(*tag-name ...*)
Deletes specific tags for the specified factor.

The *tag-name* is a 1 - 20 character identifier and can consist of alphabetic or numeric characters.

The *tag-name* is ignored when it does not already exist for a specified factor.

NOTAGS
Removes all tags for the specified factor.

ADDPOLICY | DELPOLICY

ADDPOLICY(*policy-name ...*)
Adds to the user's list of MFA authentication policies where *policy-name* is the name of an MFA policy profile defined in the MFADEF class. *Policy-name* is specified as only the unique name portion of the policy profile after the initial "POLICY." qualifier.

A policy name must be between 1 and 20 characters.

Each user is limited to a maximum of 10 policy names.

DELPOLICY(*policy-name ... | **)
Deletes the specified policies from the user's list of MFA policies.

Specifying the * character deletes all existing policies.

NOMFA
Specifies that RACF delete all MFA fields from the user's profile. The user is no longer required to provide additional authentication factors when logging on.

LISTUSER

The LISTUSER command is enhanced to support adding multi-factor information for use by IBM Multi-Factor Authentication for z/OS

Syntax

```
[ MFA ]
```

Parameters

MFA
Specifies that multi-factor authentication information should be listed for the user. The MFA keyword is ignored when NORACF is specified.

Example

```
LISTUSER USER01 MFA
USER=USER01
--------------------------------------
MULTIFACTOR AUTHENTICATION INFORMATION:
--------------------------------------
PASSWORD FALLBACK IS NOT ALLOWED
PASSWORD FALLBACK IS NOT ALLOWED
AUTHENTICATION POLICIES =
  RSAANDPASS
  TTANDPASS
FACTOR = AZFSIDP1
  STATUS = ACTIVE
  FACTOR TAGS =
    SIDUSERID:joeyuser
FACTOR = AZFTOTP1
  STATUS = ACTIVE
  FACTOR TAGS =
    REGSTATE:PROVISIONED
```

Figure 1. Example 18: Output for LISTUSER MFA when MFA information exists

RALTER

The MFA segment is intended to be updated only by IBM MFA for z/OS.

The MFPOLICY segment contains MFA authentication policy information for use by IBM MFA for z/OS.

Syntax

```
[ MFA | NOMFA ]


[ MFPOLICY(
     [ FACTORS(factor-name ...)
       | ADDFACTORS(factor-name ...)
       | DELFACTORS(factor-name ...)
       | NOFACTORS]
     [ TOKENTIMEOUT(timeout-seconds)]
     [ REUSE(YES|NO)]
     )
  | NOMFPOLICY ]
```

Parameters

MFA | NOMFA
The MFA segment is intended to be updated only by IBM Multi-Factor Authentication for z/OS.

MFA
Specifies that RACF create an MFA segment in the MFADEF profile.

NOMFA
Specifies that RACF delete the MFA segment from the MFADEF profile.

MFPOLICY | NOMFPOLICY
Specifies multi-factor authentication policy information for the MFADEF class profile being changed.

FACTORS | ADDFACTORS | DELFACTORS | NOFACTORS
Specifies the list of factors that are required to satisfy this authentication policy.

FACTORS(*factor-name1 ...*)
specifies the list of factor names that are required in order to satisfy this authentication policy.

ADDFACTORS(*factor-name1 ...*)
Adds to the list of factor names that are required in order to satisfy this authentication policy.

DELFACTORS(*factor-name1 ...*)
Deletes from the list of factor names that are required in order to satisfy this authentication policy.

NOFACTORS
Removes the list of factor names from the authentication policy.

TOKENTIMEOUT(*timeout-seconds*)
Specifies the number of seconds for which out-of-band authentication with the policy is valid. That is, after having authenticated out-of-band with the policy to IBM MFA, the user must logon to a z/OS application within this number of seconds or the out-of-band authentication record will time out. When an out-of-band authentication record times out, a user must authenticate out-of-band again to IBM MFA in order to logon.

The value of timeout-seconds can be between 1 and 86,400® (the number of seconds in a day).

The default value is 300 (5 minutes).

REUSE(YES|NO)
Specifies whether this out-of-band authentication policy allows multiple z/OS logons using the out-of-band token within the TOKENTIMEOUT setting. When REUSE(NO) is specified, the user must authenticate out-of-band with the policy prior to every z/OS logon.

REUSE(NO) is the default.

RDEFINE

The MFA segment contains factor specific multi-factor information for use by IBM MFA for z/OS.

The MFPOLICY segment contains MFA authentication policy information for use by IBM MFA for z/OS.

Syntax

```
[ MFA ]


[ MFPOLICY(
     [ FACTORS(factor-name...) ]
     [ TOKENTIMEOUT(timeout-seconds) ]
     [ REUSE(YES|NO)])
     ) ]
```

Parameters

MFA
Specifies that RACF create an MFA segment in the MFADEF class profile. The MFA segment is intended to be updated only by IBM Multi-Factor Authentication for z/OS.

MFPOLICY
Specifies multi-factor authentication policy information for the MFADEF class profile being changed.

FACTORS(*factor-name1 ...*)
Specifies the list of factor names that are required in order to satisfy the authentication policy.

TOKENTIMEOUT(*timeout-seconds*)
Specifies the number of seconds for which out-of-band authentication with the policy is valid. That is, after having authenticated out-of-band with the policy to IBM MFA, the user must logon to a z/OS application within this number of seconds or the out-of-band authentication record will time

out. When an out-of-band authentication record times out, a user must authenticate out-of-band again on IBM MFA in order to logon.

The value of timeout-seconds can be between 1 and 86,400 (the number of seconds in a day).

The default value is 300 (5 minutes).

REUSE(YES|NO)
Specifies whether this out-of-band authentication policy allows multiple z/OS logons using the out-of-band token within the TOKENTIMEOUT setting. When REUSE(NO) is specified the user must authenticate out-of-band with the policy prior to every z/OS logon.

REUSE(NO) is the default.

RLIST

A new MFA segment is added. RLIST is enhanced to display MFA information.

A new MFPOLICY segment is added. RLIST is enhanced to display MFA authentication policy information.

Syntax

```
[ MFA ]

[ MFPOLICY ]
```

Parameters

MFA
Specifies that MFA segment information should be listed for profiles in the MFADEF class.

MFPOLICY
Specifies that MFPOLICY segment information should be listed for profiles in the MFADEF class.

Examples

```
RLIST MFADEF FACTOR.FACT01 MFA
CLASS      NAME
-----      ----
MFADEF     FACTOR.FACT01

MFA INFORMATION
------------------
MFADATA is defined.
```

Figure 2. Example 16: Output for MFA segment

```
RLIST MFADEF POLICY.RSAANDPW MFPOLICY
...

MFPOLICY INFORMATION
----------------------------
FACTORS = AZFSIDP1
TOKEN TIMEOUT = 00000120
REUSE = YES
```

Figure 3. Example 17: Output for MFPOLICY segment

Chapter 7. RACF macros and interfaces for IBM MFA

This topic includes the RACF macros and interfaces that are new or changed for IBM MFA:

- RACF database unload in the record formats produced by the database unload utility.
- SMF records in the format of SMF type 80 records.
- The format of the unloaded SMF type data in the JOBINIT record extension.
- The supplied class descriptor table.
- RACF database templates in the user template for the RACF database and the general template for the RACF database.

RACF database unload for IBM MFA

User basic data record (0200)

Table 1. User basic data record

Field Name	Type	Position		Comments
		Start	End	
USBD_MFA_FALLBACK	Char	639	641	This user can use a password or password phrase to logon to the system when MFA is unavailable. Valid Values include "Yes" and "No".

User MFA factor data record (020A)

Table 2. User MFA factor data record

Field Name	Type	Position		Comments
		Start	End	
USMFA_RECORD_TYPE	Int	1	4	Record type of the user Multifactor authentication data record (020A).
USMFA_NAME	Char	6	13	User ID as taken from the profile name.
USMFA_FACTOR_NAME	Char	15	34	Factor name.
USMFA_FACTOR_ACTIVE	Date	36	54	Factor active date. Will be blank if factor is not ACTIVE.

User MFA policies record (020B)

Table 3. User MFA policies record

Field Name	Type	Position		Comments
		Start	End	
USMPOL_RECORD_TYPE	Int	1	4	Record type of the user Multi-factor authentication policies record (020B)
USMPOL_NAME	Char	6	13	User ID as taken from the profile name.
USMPOL_POLICY_NAME	Char	15	34	MFA Policy name.

User MFA factor tags data record (1210)

Table 4. User MFA factor tags data record

Field Name	Type	Position		Comments
		Start	End	
USMFAC_RECORD_TYPE	Int	1	4	Record type of the user Multifactor authentication factor configuration data record (1210).
USMFAC_NAME	Char	6	13	User ID as taken from the profile name.
USMFAC_FACTOR_NAME	Char	15	34	Factor name.
USMFAC_TAG_NAME	Char	36	55	The tag name associated with the factor.
USMFAC_TAG_VALUE	Char	57	1080	Tag value associated with the tag name.

General resource MFA factor definition record (05H0)

Table 5. General resource MFA factor definition record

Field Name	Type	Position		Comments
		Start	End	
GRMFA_RECORD_TYPE	Int	1	4	Record type of the Multifactor factor definition data record (05H0)
GRMFA_NAME	Char	6	251	General resource name as taken from the profile name.
GRMFA_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely MFADEF.
GRMFA_FACTOR_DATA_LEN	Int	262	266	Length of factor data.

General resource MFPOLICY definition record (05I0)

Table 6. General resource MFAPOLICY definition record (05I0)

Field Name	Type	Position		Comments
		Start	End	
GRMFP_RECORD_TYPE	Int	1	4	Record type of the Multifactor Policy Definition data record (05I0).
GRMFP_NAME	Char	6	251	General resource name as taken from the profile name.
GRMFP_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely MFADEF.
GRMFP_TOKEN_TIMEOUT	Int	262	271	MFA token timeout setting.
GRMFP_REUSE	Yes/No	273	275	MFA token reuse setting.

General resource MFA policy factors record (05I1)

Table 7. General resource MFA policy factors record (05I1)

Field Name	Type	Position		Comments
		Start	End	
GRMPF_RECORD_TYPE	Int	1	4	Record type of the user Multifactor authentication policy factors record (05I1).
GRMPF_NAME	Char	6	251	General resource name as taken from the profile name.
GRMPF_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely MFADEF.
GRMPF_POL_FACTOR	Char	262	281	Policy factor name.

RACF SMF records for IBM MFA

SMF record-type 80 - Event codes and event code qualifiers

New event code qualifiers are added for event code, type 80, record 1:

- 40(28) - Successful Multifactor authentication
- 41(29) - INVMFA - Failed Multifactor authentication
- 42(2A) - MFAUNAVL - Failed authentication because no multifactor decision could be made for a MFA user who has the NOPWFALLBACK option
- 43(2B) - MFAPSUCC - IBM MFA partial success: credentials were not incorrect, but a re-authentication is required

A successful MFA fallback is audited with existing event code qualifiers.

Note: A successful MFA fallback authentication will be unconditionally audited (regardless of what the application specified on LOG= and regardless of whether SETROPTS AUDIT(USER) is active.

SMF record-type 80 - Table of extended-length relocate section variable data

Table 8. Table of extended-length relocate section variable data

Data type (SMF80TP2) dec(hex)	Data length (SMF80DL2)	Format	Audited by event code	Description (SMF80DA2)
440(1B8)	8	binary	13	Byte 1: MFA subkeyword specified flags **Bit** **Meaning** **0** PWFALLBACK specified **1** NOPWFALLBACK specified **2** FACTOR specified **3** DELFACTOR specified **4** ACTIVE specified **5** NOACTIVE specified **6** TAGS specified **7** DELTAGS specified Byte 2: MFA subkeyword specified flags **Bit** **Meaning** **0** NOTAGS specified **1** ADDPOLICY specified **2** DELPOLICY specified **3-7** Reserved Bytes 3-8: Reserved for IBM's use
441(1B9)	variable	EBCDIC	13	Multifactor authentication factor name

Table 8. Table of extended-length relocate section variable data (continued)

Data type (SMF80TP2) dec(hex)	Data length (SMF80DL2)	Format	Audited by event code	Description (SMF80DA2)
442(1BA)	variable	EBCDIC	13	MFA tag entry from the TAGS/DELTAGS keyword. When TAGS is specified, the entry value is the tag name and value separated by a colon (":"). When DELTAGS is specified, the entry value is the tag name only.
443(1BB)	variable	mixed	1	Byte 1: Authentication information: **Bit** **Meaning** **0** ACEE was created from VLF cache **1** User has active MFA factor(s) **2** MFA user allowed to fall back when no MFA decision can be made **3** No MFA decision for MFA user **4** IBM MFA requested that RACROUTE REQUEST=VERIFY return the password-expired return code. **5** IBM MFA requested that RACROUTE REQUEST=VERIFY return the new-password-invalid return code. **6** IBM MFA requested that RACROUTE REQUEST=VERIFY return the password-invalid return code, but not to increment the password revoke count (partial success - needs more information). **7** Relocate 443 is extended. Byte 2: Authenticator(s) used: **Bit** **Meaning** **0** Password Evaluated **1** Password Successful **2** Password Phrase Evaluated **3** Password Phrase Successful **4** Passticket Evaluated **5** Passticket Successful **6** MFA authentication successful **7** MFA authentication unsuccessful Bytes 3-6: MFA Authorization Return Code. Bytes 7-10: MFA Authorization Reason Code

Table 8. Table of extended-length relocate section variable data (continued)

Data type (SMF80TP2) dec(hex)	Data length (SMF80DL2)	Format	Audited by event code	Description (SMF80DA2)
444 (1BC)	variable	EBCDIC	13	MFA policy name entry from the ADDPOLICY/ DELPOLICY keyword.

SMF record-type 80 - Data type 6 command-related data

The SMF Type 80 relocate section 6 (command-related data) format is updated for ALTUSER. There are currently two sets of 'keywords specified/ignored/violated' fields, the first containing 32 bits and the second containing 16 bits. These are now full. A third set of bit-string fields will be defined as 32 bits each. A pair of new bits will be defined in each for the MFA and NOMFA keywords.

Table 9. Table of data type 6 command-related data

Event code dec(hex)	Command	Data length	Format	Description
13 (D)	**ALTUSER**	4	Binary	Flags for additional keywords specified: **Bit** **Keyword specified** **Byte 0** **0** *MFA **1** *NOMFA **2-7** Reserved for IBM's use **Byte 1** **0-7** Reserved for IBM's use **Byte 2** **0-7** Reserved for IBM's use **Byte 3** **0-7** Reserved for IBM's use
		4	Binary	Flags for additional keywords ignored (authorization): **Bit** **Keyword specified** **Byte 0** **0** *MFA **1** *NOMFA **2-7** Reserved for IBM's use **Byte 1** **0-7** Reserved for IBM's use **Byte 2** **0-7** Reserved for IBM's use **Byte 3** **0-7** Reserved for IBM's use
		4	Binary	Flags for additional keywords ignored because of processing error: **Bit** **Keyword specified** **Byte 0** **0** *MFA **1** *NOMFA **2-7** Reserved for IBM's use **Byte 1** **0-7** Reserved for IBM's use **Byte 2** **0-7** Reserved for IBM's use **Byte 3** **0-7**

The JOBINIT record extension

In the unloaded SMF Type 80 record, the ALTUSER event code D (13 decimal) can have the MFA keywords appear in the "keywords specified" and "keywords failed" fields.

In addtion, the following fields are added to the unloaded JOBINIT record extension, based on information in the new extended relocate section 443 (note that the reason for MFA fallback is not unloaded).

Table 10. Format of the job initiation record extension (event code 01)

Field name	Type	Length	Position		Comments
			Start	End	
INIT_ACEE_VLF	Yes/No	4	4540	4543	The ACEE was created from the VLF cache.
INIT_MFA_USER	Yes/No	4	4545	4548	The user has active MFA factors.
INIT_MFA_FALLBACK	Yes/No	4	4550	4553	The MFA user is allowed to fall back to password authentication when IBM MFA is unavailable.
INIT_MFA_UNAVAIL	Yes/No	4	4555	4558	MFA was unavailable to make an authentication decision for the IBM MFA user.
INIT_MFA_PWD_EXPIRED	Yes/No	4	4560	4563	IBM MFA requested that RACROUTE REQUEST=VERIFY return the password-expired return code.
INIT_MFA_NPWD_INV	Yes/No	4	4565	4568	IBM MFA requested that RACROUTE REQUEST=VERIFY return the new-password-invalid return code.
INIT_MFA_PART_SUCC	Yes/No	4	4570	4573	IBM MFA requested that RACROUTE REQUEST=VERIFY return the password-invalid return code, but not to increment the password revoke count (partial success - needs more information).
INIT_RELO443_EXTENDED	Yes/No	4	4575	4578	Relocate 443 is extended.
INIT_PASSWORD_EVAL	Yes/No	4	4580	4583	The supplied password was evaluated.
INIT_PASSWORD_SUCC	Yes/No	4	4585	4588	The supplied password was evaluated successfully.
INIT_PHRASE_EVAL	Yes/No	4	4590	4593	The supplied password phrase was evaluated.
INIT_PHRASE_SUCC	Yes/No	4	4595	4598	The supplied password phrase was evaluated successfully.
INIT_PASSTICKET_EVAL	Yes/No	4	4600	4603	The supplied password was evaluated as a PassTicket.
INIT_PASSTICKET_SUCC	Yes/No	4	4605	4608	The supplied password was evaluated successfully as a PassTicket.
INIT_MFA_SUCC	Yes/No	4	4610	4613	MFA authentication successful.
INIT_MFA_FAIL	Yes/No	4	4615	4618	MFA authentication unsuccessful.
INIT_AUTH_RSN1	Char	8	4620	4627	MFA Authentication return code. Expressed as hexadecimal number.
INIT_AUTH_RSN2	Char	8	4629	4636	MFA Authentication reason code. Expressed as hexadecimal number.

RACF database templates for IBM MFA

The MFA segment is added to the GENERAL profile and the MFA fields are added to the base segment of the USER profile.

The USER template:

Table 11. The USER template, Base segment

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	
MFAFLBK	109	20	80	00000001	00		User can fall back to password logon
FACTORN	110	10	80	00000004	00		Number of defined factors
FACTOR	111	80	80	00000000	00		Factor name - repeat
FACACDT	112	82	80	00000008	FF		Factor active-on date - repeat
FACTAGS	113	80	00	00000000	00		Factor configuration data - repeat
MFAPOLN	120	10	80	00000004	00		Number of defined policies
MFAPOLNM	121	80	80	00000000	00		Policy name - repeat

The GENERAL template:

Table 12. The GENERAL template, MFA segment and MFPOLICY segment

Field name (character data)	Field ID	Flag 1	Flag 2	Field length decimal	Default value	Type	Field being described
MFA	001	00	00	00000000	00		Start of segment fields
MFDATA	002	00	00	00000000	00		Free-form factor metadata
MFPOLICY	001	00	00	00000000	00		Start of segment fields
MFFCTRN	002	10	00	00000004	00		Number of factors in policy
MFFCTRS	003	80	00	00000000	00		Policy factor list
MFTIMEO	004	00	00	00000004	00		Policy token timeout
MFREUSE	005	00	00	00000001	00		Policy reuse setting

RACF supplied class descriptor table IBM MFA

Table 13. Classes supplied by IBM

Class	Attributes	
MFADEF	POSIT=600	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
		RVRSMAC=NO
	OPER=NO	KEYQUAL=0
	PROFDEF=YES	ID=1
	FIRST=NONATNUM	CASE=UPPER
	SIGNAL=NO	
		GENERIC=ALLOWED

Chapter 8. RACF messages and codes for IBM MFA

This topic includes the RACF messages and codes that are new or changed for IBM MFA.

ALTUSER command messages

This topic describes the RACF ALTUSER messages that are affected by IBM Multi-Factor Authentication for z/OS (IBM MFA).

ICH21046I **MFA cannot be specified for PROTECTED user *user-ID*.**

Explanation

The MFA keywords are used to configure multi-factor authentication data and are not meaningful for a PROTECTED user.

System action

All MFA information is ignored. Command processing continues.

User response

Specify a different user ID, or assign the user ID a password, or preferably a password phrase.

ICH21047I **The FACTOR keyword must be specified when specifying other factor related keywords. No MFA data is updated.**

Explanation

The FACTOR operand of the MFA keyword is required when specifying ACTIVE, NOACTIVE, TAGS, DELTAGS, or NOTAGS.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Correct the command.

ICH21048I **Factor name *factor-name* cannot be added until the *profile-name* profile is created in the MFADEF class.**

Explanation

The use of a given factor is enabled for the system when the security administrator defines the factor name in the MFADEF class, in the format demonstrated by *profile-name*. This must be a discrete profile. Until the profile is defined, the factor cannot be assigned to any users.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Either correct the factor name or define the factor in the MFADEF class for system use.

ICH21049I **A maximum of *max-factor* factors can be specified for *user-ID*.**

Explanation

The command attempted to assign a factor that would exceed the limit of *max-factor* factors for the noted user.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Either correct the factor name or remove a different factor from the user's profile.

ICH21050I **A maximum of *max-tag* tags can be specified for factor *factor-name* and user *user-ID*.**

Explanation

The command attempted to assign a tag that would exceed the limit of *max-tag* tags for the specified factor name and user-ID.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Either correct the tag name or remove a different tag from the factor definition in the user's profile.

ICH21051I **IBM MFA detected an error in the *name-or-value* of tag *tag-name* with the following message: *MFA-msg***

Explanation

RACF contacted IBM MFA to validate the tag name and value specified, and IBM MFA reflected an error as described in the text of *MFA-msg*. If no message is returned, *MFA-msg* will contain the string "*No message returned*".

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

For more information, see the message description in *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH21052I **Unable to contact MFA to validate tag data. No MFA data is updated.**

Explanation

RACF could not contact IBM MFA to validate the tag name(s) and value(s) specified. RACF uses a PC service to pass the tag data to IBM MFA. IBM MFA provides the PC number using a name/token pair. RACF received a non-zero return code when using the IEANTRT service to obtain the PC value.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Ensure that IBM MFA address space is active and has been configured properly. For more information, see *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH21053I **Unexpected error return code=*return-code* and reason code=*reason-code* from IBM MFA while processing user *user-id*.**

Explanation

RACF encountered an unexpected error from IBM Multi-Factor Authentication for z/OS while attempting to validate the tag name(s) and value(s) specified. RACF uses a PC service to pass the tag data to IBM MFA. The IBM MFA PC returned unexpected codes.

System action

All MFA information is ignored, including fields that are not factor-specific. Command processing continues.

User response

Ensure that IBM MFA address space is active and has been configured properly. For more information, see *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH21054I **Factor *factor-name* for user *user-ID* contains tag data which is not valid. Use the NOTAGS operand to remove the tag data.**

Explanation

The tag data associated with the specified factor and user in the RACF database is not valid.

System action

All MFA information is ignored for the specified user, including fields that are not factor-specific. Command processing continues.

User response

Use the ALTUSER command with the NOTAGS operand to remove the tag data that is not valid. For example, issue the following command: ALTUSER *user-ID* MFA(FACTOR(*factor-name*) NOTAGS).

ICH21055I **Unable to notify IBM MFA of tag deletion for user *user-ID* and factor *factor-name*. Tag data is deleted.**

Explanation

RACF attempted to notify IBM Multi-Factor Authentication for z/OS for the deletion of tag data, but the notification failed. RACF uses a PC service to pass the tag data to IBM MFA. IBM MFA provides the

PC number using a name/token pair. RACF received a non-zero return code when using the IEANTRT service to obtain the PC value.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

Determine the problem with IBM Multi-Factor Authentication for z/OS.

ICH21056I **Error during notification of IBM MFA for deletion of tag *tag-name* for user *user-ID* and factor *factor-name* with the following message: *MFA-msg***

Explanation

RACF contacted IBM Multi-Factor Authentication for z/OS to delete the tag name noted in the message, and IBM MFA reflected an error as described in the text of *MFA-msg*. If no message is returned, *MFA-msg* will contain the string "*No message returned*".

Note: The maximum length of this message is 252 characters. If all of the inserts are very long, *MFA-msg* may be truncated to fit into 252 characters.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

For more information, see the message description in *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH21057I **Unexpected return code=*return-code* and reason code=*reason-code* from IBM MFA during tag deletion notification for user *user-id* and factor *factor-name*. Tag data is deleted.**

Explanation

RACF encountered an unexpected error from IBM Multi-Factor Authentication for z/OS while attempting to notify IBM MFA that tag data has been deleted for the user and factor noted in the message. RACF uses a PC service to pass the tag data to IBM MFA. The IBM MFA PC returned unexpected return codes.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

Determine the problem with IBM Multi-Factor Authentication for z/OS.

ICH21058I **Factor *factor-name* for user *user-ID* contains tag data which is not valid. Tag data is deleted and IBM MFA is not notified.**

Explanation

While deleting tag data for the specified factor and user, RACF detected tag data which is not valid. IBM Multi-Factor Authentication for z/OS is usually notified when tag data is deleted; since the tag data is not valid, notification to IBM MFA is not attempted.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

No further action is required.

ICH21059I **A maximum of *max-policies* policy names can be specified. *Policy-name* not added to user *userid*.**

Explanation

The *policy-name* policy is ignored.

System action

Command processing stops with no update to the user.

User response

Remove an existing policy before attempting to add another policy.

DELUSER command messages

This topic describes the RACF DELUSER messages that are affected by IBM Multi-Factor Authentication for z/OS (IBM MFA).

ICH04019I **Unable to contact IBM MFA of tag deletion for user *user-id* and factor *factor-name*. Tag data is deleted.**

Explanation

RACF attempted to notify IBM Multi-Factor Authentication for z/OS for the deletion of tag data, but the notification failed. RACF uses a PC service to pass the tag data to IBM MFA. IBM MFA provides the PC number using a name/token pair. RACF received a non-zero return code when using the IEANTRT service to obtain the PC value.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

Determine the problem with IBM Multi-Factor Authentication for z/OS.

ICH04020I **Error during notification of IBM MFA for deletion of tag *tag-name* for user *user-ID* and factor *factor-name* with the following message: *MFA-msg***

Explanation

RACF contacted IBM Multi-Factor Authentication for z/OS to delete the tag name noted in the message, and IBM MFA reflected an error as described the text of *MFA-msg*. If no message is returned, *MFA-msg* will contain the string "'*No message returned*'".

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

For more information, see the message description in *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH04021I **Unexpected return code=*return-code* and reason code=*reason-code* from IBM MFA during tag deletion notification for user *user-id* factor *factor-name*. Tag data is deleted**

Explanation

RACF encountered an unexpected error from IBM Multi-Factor Authentication for z/OS while attempting to notify IBM MFA that tag data has been deleted for the user and factor noted in the message. RACF uses a PC service to pass the tag data to IBM MFA. The IBM MFA PC returned unexpected return codes.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

Determine the problem with IBM Multi-Factor Authentication for z/OS.

ICH04022I **Factor *factor-name* for user *user-ID* contains tag data which is not valid. Tag data is deleted and IBM MFA is not notified.**

Explanation

While deleting tag data for the specified factor and user, RACF detected tag data which is not valid. IBM Multi-Factor Authentication for z/OS is usually notified when tag data is deleted; since the tag data is not valid, notification to IBM MFA is not attempted.

System action

The tag data is deleted from the RACF database. Command processing continues.

User response

No further action is required.

LISTUSER command messages

This topic describes the RACF LISTUSER messages that are affected by IBM Multi-Factor Authentication for z/OS (IBM MFA).

ICH30016I **Tag data is not valid. Use the ALTUSER command with the NOTAGS operand to remove the tag data.**

Explanation

The tag data in the RACF database associated with the user and factor currently being displayed is not valid.

System action

The tag data is not displayed for the user and factor. Command processing continues.

Problem determination

Use the ALTUSER command with the NOTAGS operand to remove the tag data that is not valid. For example, issue the following command: ALTUSER *user-ID* MFA(FACTOR(*factor-name*) NOTAGS).

Dynamic parse messages

This topic describes the RACF dynamic parse messages that are affected by IBM Multi-Factor Authentication for z/OS (IBM MFA).

IRR52221I ***keyword-name* is intended to be updated only by IBM MFA. Command processing terminated.**

Explanation

The named keyword in the MFA segment is not allowed to be specified by RACF commands. Some fields in the MFA segment are intended to be updated only by IBM MFA.

System action

Command processing ends.

User response

Correct the command.

RACROUTE REQUEST=VERIFY operator messages

This topic describes the RACF RACROUTE REQUEST=VERIFY messages that are affected by IBM Multi-Factor Authentication for z/OS (IBM MFA).

ICH70008I **IBM MFA Message: *mfa-message***

Explanation

RACROUTE REQUEST=VERIFY received message text from IBM MFA while processing a request to authenticate a user with an active MFA factor.

System action

For the information you need to evaluate the *mfa-message* and take the appropriate action, see *IBM Z Multi-Function Authentication User's Guide*, which is available at the IBM Z Multi-Factor Authentication documentation (www.ibm.com/docs/en/zma) website.

ICH408I **LOGON/JOB INITIATION - MULTIFACTOR AUTHENTICATION [FAILURE | UNAVAILABLE]**

Explanation

Either of the following problems has occurred:

- A user with active multifactor authentication factors attempted to log on with invalid credentials as determined by IBM Multi-Factor Authentication for z/OS.
- A user with active multifactor authentication factors attempted to log on, but either IBM Multi-Factor Authentication for z/OS was unavailable to verify them, or RACF was unable to contact IBM MFA. The user is not allowed to fall back to the use of a password or password phrase. The SMF record contains additional information regarding the unavailability of IBM MFA.

System action

RACF prevents the user from logging on.

User response

Correct any errors in the credentials and try again.

If the problem persists, contact a system administrator.

Chapter 9. RACF RACROUTE Macros for IBM MFA

RACF RACROUTE REQUEST=VERIFY and REQUEST=VERIFYX parameters

RACF RACROUTE Macros for IBM MFA has been updated to include updates for the RACF support for IBM MFA.

,PASSCHK=YES
,PASSCHK=NO
,PASSCHK=NOMFA

specifies whether the user's password, password phrase, MFA credentials, OIDCARD, or Identity Token (IDT) is to be verified.

YES

RACROUTE REQUEST=VERIFY verifies the user's password, password phrase, MFA credentials, OIDCARD , or IDT.

There are some circumstances where verification does not occur even though PASSCHK=YES is specified. Some examples are surrogate processing (see *z/OS Security Server RACF Security Administrator's Guide*) or when the START or the ENVRIN keywords are specified.

A user ID with the protected attribute can be authenticated with PASSCHK=YES with an IDT when the covering IDTDATA profile indicates PROTALLOWED(YES). See the Identity Token Area (mapped by SAF macro IRRPIDTA) and *z/OS Security Server RACF Command Language Reference* for more details on the RACF IDT support.

For a user subject to multi-factor authentication (MFA), RACF passes the contents of the PASSWRD=, NEWPASS=, PHRASE=, and NEWPHRASE= keywords to the MFA started task, where they are evaluated as MFA credentials. If the credentials are unable to be evaluated as MFA credentials (for example, if the MFA started task is unavailable), they are evaluated as RACF credentials if the user is allowed to fall back to password-based authentication.

NO

The user's password, password phrase, MFA credentials, OIDCARD, or IDT is not verified. And, if the logon is successful, no message is issued. The IDTA keyword will be ignored and any supplied IDT will be ignored and no IDT will be generated.

NOMFA

Same as YES, except password and password phrase parameters are always verified as a password or password phrase, not as MFA credentials, even for users who have an active MFA factor.

Use of the PASSCHK=NOMFA parameter requires that RELEASE=1.9 or later be specified.

RACF RACROUTE REQUEST=VERIFY and REQUEST=VERIFYX return codes and reason codes

A new RACROUTE REQUEST=VERIFY return code and reason code has been added for the RACF support for IBM MFA.

08

Requested function has failed.

RACF RC
Meaning

68

Indicates that an error occurred while processing an MFA request.

Reason Code
Meaning

0004yyyy

An error occurred while RACROUTE REQUEST=VERIFY was processing the results of an MFA authentication request. "yyyy" contains diagnostic data.

Chapter 10. RACF API's for IBM MFA

This topic includes the RACF callable services that are new or changed for IBM MFA:

- The R_Admin topic is updated to add new MFA fields
- The R_Factor topic is new
- The R_Gensec topic is updated to add a new function code
- The R_Ticketserv topic is updated to add a new Ticket_options value

R_Admin (IRRSEQ00): Authentication Factor Service

The R_Admin reference is updated to include fields for the RACF support for IBM MFA:

- The table for BASE segment fields is updated to add the MFA fields.
- The table for MFA segment fields is added.
- The table for MFPOLICY segment fields is added.

BASE segment fields

Table 14. BASE segment fields

Field name	SAF field name	Flag byte values	ADDUSER/ALTUSER keyword Reference, or LISTUSER heading (for output-only fields)	Allowed on add requests	Allowed on alter requests	Returned on extract requests
FACTORN		N/A	**Note:** This is the list header field for the 42-dimensional array consisting of the following three fields (see the factor tags notes that follow).	No	No	Yes
FACTOR		'Y'	MFA(FACTOR(xx))	No	Yes	Yes
		'D"	MFA(DELFACTOR(xx))	No	Yes	Yes
FACACTV (boolean)		'Y'	MFA(ACTIVE)	No	Yes	Yes
		'N'	MFA(NOACTIVE)	No	Yes	Yes
FACTAGnn		N/A	FACTOR TAGS =	No	No	Yes
FACVALnn		N/A	FACTOR TAGS =	No	No	Yes
MFAFLBK (boolean)		'Y'	MFA(PWFALLBACK)	No	Yes	Yes
		'N'	MFA(NOPWFALLBACK)	No	Yes	
MFAPOLNM (list MFAPOLN)		'A'	MFA(ADDPOLICY(xx ...))	No	Yes	Yes
		'D'	MFA(DELPOLICY(xx ...))	No	Yes	

Notes for MFA:

- The MFA fields FACTORN (including subfields), MFAPOLNM, and MFAFLBK are represented differently on input (ADMN_ALT_USER) vs. output (ADMN_XTR_USER). For ADMN_ALT_USER, see User administration in *z/OS Security Server RACF Callable Services*.

- On output for a multi-factor authentication user, each tag is represented using separate fields for the tag name and tag value (for example, FACTAG01 contains the name of the first tag and FACVAL01 contains the value of the first tag). Twenty pairs of these fields are returned for every MFA user, regardless of how many tags actually exist. A non-zero length indicates the actual existence of the tag in the user profile.

MFA segment fields

Table 15. MFA segment fields

Field name	SAF field name	Flag byte values	ALTUSER keyword reference	Allowed on add requests	Allowed on alter requests	Returned on extract requests
FACTOR		'Y'	MFA(FACTOR(xx))	No	Yes	Yes
		'D'	MFA(DELFACTOR(xx))	No	Yes	Yes
FACACTV (boolean)		'Y'	MFA(ACTIVE)	No	Yes	Yes
		'N'	MFA(NOACTIVE)	No	Yes	Yes
FACTAGS		'Y'	MFA(TAGS(xx ...))	No	Yes	No
		'D'	MFA(DELTAGS(xx ...))	No	Yes	No
		'N'	MFA(NOTAGS)	No	Yes	No
MFAFLBK (boolean)		'Y'	MFA(PWFALLBACK)	No	Yes	Yes
		'N'	MFA(NOPWFALLBACK)	No	Yes	
MFAPOLNM (list MFAPOLN)		'A'	MFA(ADDPOLICY(xx ...))	No	Yes	Yes
		'D'	MFA(DELPOLICY(xx ...))	No	Yes	

Notes:

- For the ADMN_ALT_USER function, MFA fields are treated as a non-BASE segment even though the fields reside in the BASE segment of the user profile.
- For the ADMN_XTR_USER function, MFA fields are returned in the BASE segment.

MFPOLICY segment fields

Table 16. MFPOLICY segment fields

Field name	SAF field name	Flag byte values	RDEFINE/RALTER keyword reference	Allowed on add requests	Allowed on alter requests	Returned on extract requests
FACTORS (list FACTORS)		'Y'	MFPOLICY(FACTORS(xx ...))	Yes	Yes	Yes
		'A'	MFPOLICY(ADDFACTORS(xx ...))	No	Yes	
		'D'	MFPLICY(DELFACTORS(xx ...))	No	Yes	
		'N'	MFPOLICY(NOFACTORS))	No	Yes	
TIMEOUT		'Y	MFPOLICY(TOKENTIMEOUT(xx))	Yes	Yes	Yes
REUSE (boolean)		'Y'	MFPOLICY(REUSE(YES))	Yes	Yes	Yes
		'N'	MFPOLICY(REUSE(NO))	Yes	Yes	

R_factor (IRRSFA64): Authentication Factor Service

Function

The **R_Factor** service provides functions required by multi-factor authentication applications to store and retrieve associated data in the RACF database.

1. Get general factor data
2. Set general factor data
3. Get user factor data
4. Set user factor data
5. Get general policy data
6. Get cached token credential

Requirements

Authorization:
Any PSW key in supervisor or problem state

Dispatchable unit mode:
Task or user

Cross memory mode:
PASN = HASN

AMODE:
64

RMODE:
Any

ASC mode:
Primary or AR mode

Recovery mode:
ESTAE. Caller cannot have an FRR active.

Serialization:
Enabled for interrupts

Locks:
No locks held

Control parameters:
The parameter list and the work area must be in the primary address space. The words containing ALETs must be in the primary address space. The Num_parms parameter must be in the primary address space.

Linkage conventions

Callers in 64-bit addressing mode should link-edit the IRRSAF64 stub module with their code and use the IRRPCOMY mapping macro.

RACF authorization

Callers running in system key or supervisor state may specify any function code.

Non-system key problem-state callers require the following authorization for each function code:

1. Get general factor data

   Read access to the resource IRR.RFACTOR.MFADEF.*factorName* in the FACILITY class, where *factorName* matches a profile defined in the MFADEF class.

2. Set general factor data

   Read access to the resource IRR.RFACTOR.MFADEF.*factorName* in the FACILITY class, where *factorName* matches a profile defined in the MFADEF class.

3. Get user factor data

   Read access to the resource IRR.RFACTOR.USER in the FACILITY class.

4. Set user factor data

   Update access to the resource IRR.RFACTOR.USER in the FACILITY class

5. Get policy data

   Read access to the resource IRR.RFACTOR.MFADEF.*policyName* in the FACILITY class, where *policyName* matches a profile defined in the MFADEF class.

6. Get cached token credential (CTC)

   READ access to the resource IRR.RFACTOR.GETCTC in the FACILITY class.

Format

```
CALL IRRSFA64   (Work_area,
                 ALET, SAF_return_code,
                 ALET, RACF_return_code,
                 ALET, RACF_reason_code,
                 Num_parms,
                 Parm_ALET, Function_code,
                            Function_parmlist
                )
```

Parameters

Work_area
The name of a 1024-byte work area for SAF. The work area must be in the primary address space.

ALET
The name of a word containing the ALET for the following parameter. Each parameter must have an ALET specified. The words containing the ALETs must be in the primary address space.

SAF_return_code
The name of a fullword in which the SAF router returns the SAF return code.

RACF_return_code
The name of a fullword in which the service routine stores the return code.

RACF_reason_code
The name of a fullword in which the service routine stores the reason code.

Num_parms
Specifies the name of a fullword that contains the total number of parameters in the parameter list. The contents of this field must be set to eleven (x'0000000B').

Parm_ALET
The name of a word containing the ALET for all the parameters that follow, including function code specific parameter lists and areas referenced from them.

Function_code
The name of a 2-byte area containing the function code. The function code has one of the following values:

x'0001' - Get general factor data
x'0002' - Set general factor data
x'0003' - Get user factor data
x'0004' - Set user factor data
x'0005' - Get general policy data
x'0006' - Get cached token credential

Function_parmlist

Specifies the name of the function code specific parameter list area for the function_code specified.

All address fields are 8-byte addresses. When referring to 31-bit storage addresses, the caller must make sure that the high-order word of the address field is set to binary zeros.

Table 17. Function parmlist for x'0001' - Get general factor data

Offset	Length	Name	Description
0	0	FACT_GETF_PLIST	Name of structure.
0	4	FACT_GETF_OPTIONS	Reserved. Must be initialized to zeroes.
4	4	FACT_GETF_FACT_LENGTH	Length (in bytes) of the factor name.
8	8	FACT_GETIF_FACTOR@	Address of the factor name.
16	4	*	Reserved. Must be initialized to zeroes.
20	4	FACT_GETF_AF_LENGTH	Length (in bytes) of free-form application data area.
24	8	FACF_GETF_AF@	Address of free-form application data area. The area must be pre-allocated by the caller and its size specified in FACT_GETF_AF_LENGTH.

Table 18. Function parmlist for x'0002' - Set general factor data

Offset	Length	Name	Description
0	0	FACT_SETF_PLIST	Name of structure.
0	4	FACT_SETF_OPTIONS	Reserved. Must be initialized to zeros.
4	4	FACT_SETF_FACTOR_ LENGTH	Length (in bytes) of the factor name.
8	8	FACT_SETF_FACTOR@	Address of the factor name.
16	4	*	Reserved. Must be initialized to zeros.
20	4	FACT_SETF_AF_LENGTH	Length (in bytes) of free-form application data area. Must not exceed 4096. Specify 0 to delete the current value.
24	8	FACT_SETF_AF@	Address of free-form application data area. The area must be pre-allocated by the caller and its size specified in FACT_SETF_AF_LENGTH.

Table 19. Function parmlist for x'0003' - Get user factor data

Offset	Length	Name	Description
0	0	FACT_GETU_PLIST	Name of structure.
0	4	FACT_GETU_OPTIONS	x'00000000' – Return application data area only. x'80000000' – Return FACT_UFT_POL in FACT_GETU_UF@.
4	4	FACT_GETU_UF_COUNT	Number of user factors. Must be initialized to zero.

Table 19. Function parmlist for x'0003' - Get user factor data (continued)			
Offset	**Length**	**Name**	**Description**
8	4	*	Reserved. Must be initialized to zero.
12	4	FACT_GETU_UF_LENGTH	Total length (in bytes) of the user factor area, a contiguous block of storage for the user factor list, user factor field lists, user factor tag lists, and other variable-length data referenced by those lists.
16	8	FACT_GETU_UF@	Address of user factor area (see FACT_UF_ENTRY). The area must be pre-allocated by the caller and its size specified in FACT_GETU_UF_LENGTH.
24	1	FACT_GETU_USER_ LENGTH	Length of User ID. Value must be from 1 to 8.
25	8	FACT_GETU_USER	User ID, which is padded with blanks.
33	1	FACT_GETU_FALL_BACK	Value must be initialized to zero. On output, value may be -- x'01' - User can fall back x'02' - User cannot fall back
34	14	*	Reserved
48	4	FACT_GETU_POL_COUNT	Number of policies.
52	4	FACT_GETU_POL_OFFSET	Offset to policy list in the user factor area (FACT_GETU_UF@).

Table 20. Function parmlist for x'0004' - Set user factor data			
Offset	**Length**	**Name**	**Description**
0	0	FACT_SETU_PLIST	Name of structure.
0	4	FACT_SETU_OPTIONS	Reserved. Must be initialized to zeroes.
4	4	FACT_SETU_UF_COUNT	Number of user factors. No more than 10 factors may be defined in the user profile.
8	4	*	Reserved. Must be initialized to zero.
12	4	FACT_SETU_UF_LENGTH	Total length (in bytes) of the user factor area, a contiguous block of storage for the user factor list, user factor field lists, user factor tag lists, and other variable-length data referenced by those lists.
16	8	FACT_SETU_UF@	Address of user factor area (see FACT_UF_ENTRY). The area must be pre-allocated by the caller and its size specified in FACT_SETU_UF_LENGTH.
24	1	FACT_SETU_USER_LENGTH	Length of User ID.
25	8	FACT_SETU_USER	User ID, which is padded with blanks.
33	1	FACT_SETU_FALL_BACK	The value must be x'00' indicating no change to the current setting.

Table 21. Function parmlist for x'0005' - Get general policy data

Offset	Length	Name	Description
0	0	FACT_GETP_PLIST	Name of structure.
0	4	FACT_GETP_OPTIONS	Reserved. Must be initialized to zeros.
4	4	FACT_GETP_POLICY_LENGTH	Length (in bytes) of the policy name.
8	8	FACT_GETP_POLICY@	Address of the policy name.
16	4	FACT_GETP_FL_COUNT	Number of policies. The policy entries start at FACT_GETP_PA@ and mapped by FACT_PF_ENTRY.
20	4	FACT_GETP_PA_LENGTH	Length (in bytes) of the policy list.
24	8	FACT_GETP_PA@	Address of the policy list.
32	4	FACT_GETP_TIMEOUT	Token time-out value in seconds.
36	1	FACT_GETP_REUSE	Token reuse setting. x'01' - Token can be reused x'02' - Token cannot be reused
37	15	*	Reserved. Must be initialized to zeroes.

Table 22. Function parmlist for x'0006' - Get cached token credential (CTC)

Offset	Length	Name	Description
0	0	FACT_GETC_PLIST	Name of structure
0	4	FACT_GETC_OPTIONS	Reserved. Must be initialized to zeroes.
4	1	FACT_GETC_USER_LENGTH	Length of User ID.
5	8	FACT_GETC_USER	User ID, which is padded with blanks.
13	8	FACT_GETC_APPL	Application name, which is padded with blanks. Optional. Set to all blanks when not supplied.
21	7	*	Reserved. Must be initialized to zeroes.
28	4	FACT_GETC_CRED_LIST_NUM	Number of credentials in the credential list. Optional. Set to 0 to generate without credentials. Maximum number of credentials is 10.
32	8	FACT_GETC_CRED_LIST@	Address of the Credential_list. The credential ist is mapped by FACT_CRED_LIST.
40	8	FACT_GETC_CTC@	Output CTC area address. Area must be preallocated and 8 bytes in length.
48	4	FACT_GETC_POLICY_LEN	Length of MFA Policy Name. Optional. Set to 0 for default policy name. Maximum MFA Policy Name length is 20.
52	20	FACT_GETC_POLICY_NAME	MFA policy name, which is padded with blanks.

Table 22. Function parmlist for x'0006' - Get cached token credential (CTC) (continued)			
Offset	**Length**	**Name**	**Description**
72	16	*	Reserved. Must be initialized to zeroes.

Policy factor list

Located at the beginning of the policy area referenced by FACT_GETP_PA@, this list is the contiguous set of policy entries, each mapped by FACT_PF_ENTRY. The number of entries is specified by FACT_GETP_FL_COUNT.

Table 23. Policy factor list			
Offset	**Length**	**Name**	**Description**
0	0	FACF_PF_ENTRY	Name of structure.
0	4	FACT_PF_FACTOR_LENGTH	Length of factor name.
4	4	FACT_PF_FACTOR_OFFSET	Positive offset from start of policy area to factor name.
8	8	*	Reserved.

User policy list

Located at the beginning of the user factor area referenced by FACT_GETU_UF@, this list is the contiguous set of policy entries, each mapped by FACT_UP_ENTRY. The number of entries is specified by FACT_GETU_POL_COUNT.

Table 24. User policy list			
Offset	**Length**	**Name**	**Description**
0	0	FACT_UP_ENTRY	Name of structure.
0	4	FACT_UP_POLICY_LENGTH	Length of policy name.
4	4	FACT_UP_POLICY_OFFSET	Positive offset from the start of policy area to policy name.
8	8	*	Reserved.

User factor list

Located at the beginning of the user factor area referenced by FACT_GETU_UF@ or FACT_SETU_UF@, this list is the contiguous set of user factor entries, each mapped by FACT_UF_ENTRY. The number of entries is specified by FACT_GETU_UF_COUNT or FACT_SETU_UF_COUNT.

Table 25. User factor list			
Offset	**Length**	**Name**	**Description**
0	0	FACT_UF_ENTRY	Name of structure mapping.
0	4	FACT_UF_FACTOR_ LENGTH	Length of factor name.
4	4	FACT_UF_FACTOR_OFFSET	Positive offset from FACT_GUTU_UF@ or FACT_SETU_UF@ to the factor name. The factor profile must already exist.
8	4	FACT_UF_FIELDS_COUNT	Number of fields for this factor.

Table 25. User factor list (continued)			
Offset	**Length**	**Name**	**Description**
12	4	FACT_UF_FIELDS_OFFSET	Positive offset from FACT_GETU_UF@ or FACT_SETU_UF@ to the user factor field list, is mapped by FACT_UFF_ENTRY

User factor field list

Located at offset FACT_UF_FIELDS_OFFSET from the beginning of the user factor area, this list is a contiguous set of user factor fields entries, each mapped by FACT_UFF_ENTRY. The number of entries is specified by FACT_UF_FIELDS_COUNT in the associated factor entry.

Table 26. User factor field list			
Offset	**Length**	**Name**	**Description**
0	0	FACT_UFF_ENTRY	Name of structure mapping.
0	4	FACT_UFF_FIELD_ID	Numeric identifier of the user field to update. Constant values for field identifiers are defined in IRRPCOMY. • FACT_FID_TAGS (variable len) - User factor tag list, FACT_UFT_LIST • FACT_FID_ACTIVE (19 bytes) - User factor active date (UTC) • FACT_FID_POLICIES (variable len) – User policies, FACT_UFT_POL
4	4	FACT_UFF_VALUE_ LENGTH	Length of the user factor field value. For function code 4, specify 0 to reset the field to its default value.
8	4	FACT_UFF_VALUE_OFFSET	Positive offset from FACT_GETU_UF@ or FACT_SETU_UF@ to the user factor field value.

User factor tag list

The user factor tag list begins with a 2-byte header (FACT_UFT_HEADER) which must be initialized to zero. The subsequent fields (FACT_UFT_PAIR_LENGTH through FACT_UFT_VALUE) are repeated as a group for each tag/value pair in the list.

For function code 4, if the tag already exists for the factor, the tag and value are replaced; unless the specified value length is zero, in which case they are deleted. If the tag does not exist in the database and its value length is nonzero, it is added. No more than 20 tags may be specified per user factor.

Table 27. User factor tag list			
Offset	**Length**	**Name**	**Description**
0	0	FACT_UFT_LIST	Name of structure mapping.
0	2	FACT_UFT_HEADER	Reserved. Must be zero.
2	2	FACT_UFT_PAIR_LENGTH	Total length of this tag/value pair entry, not including the length of this field.
4	2	FACT_UFT_TAG_ ATTRIBUTE	Tag attributes.

Table 27. User factor tag list (continued)			
Offset	**Length**	**Name**	**Description**
6	2	FACT_UFT_TAG_LENGTH	Length of tag.
8	var	FACT_UFT_TAG	Tag name.
*	2	FACT_UFT_VALUE_ LENGTH	Length of value. The length may not exceed 1024.
*	var	FACT_UFT_VALUE	Value associated with tag. Type is EBCDIC character data.

User factor active date

The user factor active date is the time after which the factor is considered 'active' for the user. Prior to this time, the user is not required to authenticate with the factor in order to logon to the system.

On input for function 4, the active date may be specified in one of the following ways:

- The 7-character keyword 'CURRENT', which stores the current UTC time.
- A length of zero (FACT_UFF_VALUE_LENGTH = 0), which clears any existing value from the user profile, resulting in the 'noactive' default.

On output for function 3, the service returns a 19-character UTC time of the format 'yyyy-mm-dd hh:mm:ss' if set in the user profile. The service does not return an active date field if the value was cleared or never set.

Credential List

The credential list is a list of authentication credentials for a user. The FACT_CRED_LIST structure repeats for each credential. The total length of all credentials combined must be no greater than 8192 bytes.

Table 28. Credential list			
Offset	**Length**	**Name**	**Description**
0	0	FACT_CRED_LIST	Name of structure mapping.
0	20	FACT_CRED_TYPE	Type of credential. Credential type is the factor name for the input credential value.
20	4	FACT_CRED_LENGTH	Credential value length. Length must be at least 1 byte and no more than 8192 bytes.
24	8	FACT_CRED_VAL_PTR	Pointer to Credential value.
32	16	*	Reserved. Must be set to zero.

Return and reason codes

IRRSFA64 returns the following values in the reason and return code parameters:

SAF return code	RACF return code	RACF reason code	Explanation
0	0	0	Successful completion.
4	0	0	RACF not installed.
8	8	4	An internal error has occurred during RACF processing.
8	8	8	Unable to establish recovery.

SAF return code	RACF return code	RACF reason code	Explanation
8	8	12	Caller is not authorized.
8	8	16	MFADEF class not active.
8	8	20	IBM MFA unavailable.
8	8	24	Error calling IBM MFA.
8	12	4	Factor not defined.
8	12	8	User not defined.
8	12	12	Policy not found.
8	16	n	A RACF ICHEINTY error occurred while retrieving data. The reason code may be useful to IBM service.
8	20	n	A RACF ICHEINTY error occurred while storing data. The reason code may be useful to IBM service. Reason code 40 indicates that adding all factor data would cause the maximum profile size to be exceeded. The data for one or more specified factors was not stored.
8	24	0	A tag list error has been detected in the data base.
8	24	4	Too many tags for the user factor.
8	24	8	Too many factors for the user.
8	30	n	An unexpected logic error has been encountered. The reason code may be useful to IBM service.
8	20	n	Error saving data from the data base.
8	100	n	A parameter list error has been detected. The RACF reason code identifies the parameter in error. The reason code is the ordinal position.
8	104	n	A function-specific parameter list (pointed to by the function_parmlist parameter) error has been detected. The RACF reason code identifies the offset of the field in error.
8	108	n	A factor list error has been detected. The reason code is one of the following: 0 - The offset to the factor name plus its length extends beyond the user factor area. 4 - The offset to the user factor field entry plus its length extends beyond the user factor area. 8 - Too many fields specified for the factor. 12 - The factor name is too long.

SAF return code	RACF return code	RACF reason code	Explanation
8	112	n	A factor list error has been detected. The reason code is one of the following: 0 - The offset to the factor name plus its length extends beyond the user factor area. 4 - The field identifier is not supported. 8 - A tag list error has been detected. 12 - An active date error has been detected. The value must be the 7-character keyword *CURRENT* to set the current UTC time, or have a length of zero to clear the existing value in the user profile.
8	116	n	A tag list error has been detected.
8	120	n	Supplied buffer is too small. The reason code identifies the buffer length field, which the service updated with the minimum required length. 10 - FACT_GETF_AF_LENGTH 30 - FACT_GETU_UF_LENGTH 50 - FACT_GETP_PA_LENGTH
8	124	n	IBM MFA has detected an error. The reason code is one of the following: 0 - User ID not defined. 1 - User does not have an authentication policy. 2 - Credential List error. Credential type not valid. 3 - Credential List error. Credential length not valid. 4 - Credential List error. Error parsing credential. 5 - Policy name error.
8	128	0	Credentials invalid for user.
8	132	n	IBM MFA has encountered an error extracting MFA data from the user profile. The reason code may be helpful to IBM service.
8	136	n	IBM MFA has encountered a parameter error. The reason code may be helpful to IBM service.
8	140	n	IBM MFA has encountered a parameter error. The reason code may be helpful to IBM service.
8	144	n	IBM MFA has encountered an internal error. The reason code may be helpful to IBM service.

SAF return code	RACF return code	RACF reason code	Explanation
8	148	n	IBM MFA has encountered an unknown error. The reason code may be helpful to IBM service.

Parameter List Example - Get user factor data

The R_factor caller must allocate storage for the areas shown, and must properly set input values in the primary and function-specific parameter lists. The service will return data in the user factor area, as shown in the following example.

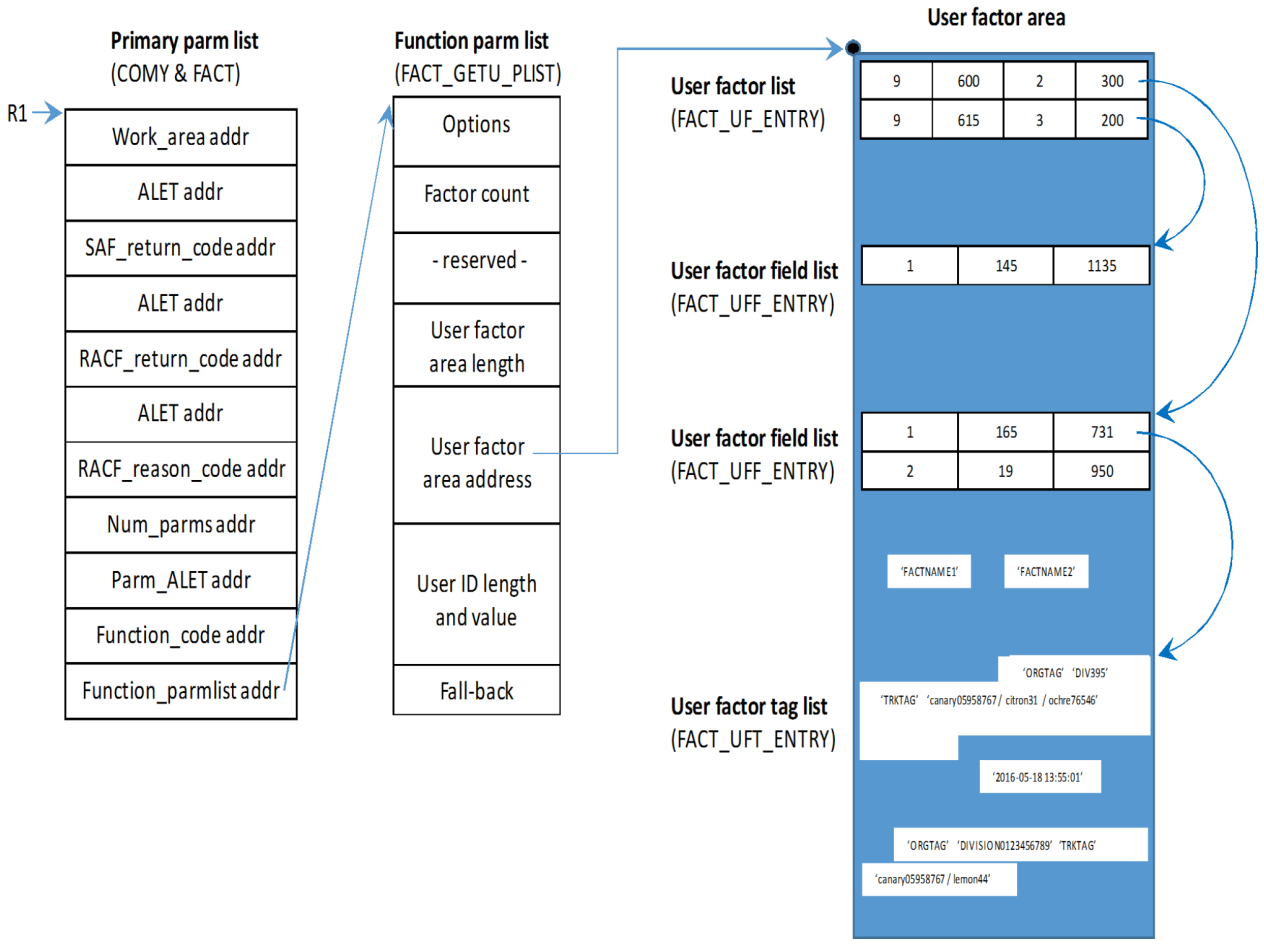

Figure 4. Parameter List Example – Get user factor data

R_GenSec (IRRSGS00 or IRRSGS64): Generic security API interface

R_Gensec is updated to add a new PassTicket Subfunction code value:

- 3 - Evaluate PassTicket Extended

When Subfunction code 3 is provided, instead of receiving a RACF return code of 16 and a RACF reason code of 32 for an unsuccessful PassTicket evaluation, the following will be returned instead:

SAF return code	RACF return code	RACF reason code	Explanation
8	16	X'nnnnnnnn'	PassTicket evaluation extended failure. X'nnnnnnnn' is the internal reason code for the evaluation failure.

R_TicketServ (IRRSPK00): Parse or extract

The R_TicketServ Ticket_options parameter is updated to add a new value to indicate that the PassTicket failure reason code should be returned.

- X'00000003' - Evaluate a PassTicket Extended

When Ticket_options 3 is provided, instead of receiving a RACF return code of 16 and a RACF reason code of 32 for an unsuccessful PassTicket evaluation, the following will be returned instead:

SAF return code	RACF return code	RACF reason code	Explanation
8	16	X'nnnnnnnn'	PassTicket evaluation extended failure. X'nnnnnnnn' is the internal reason code for the evaluation failure.

Appendix A. Accessibility

Accessible publications for this product are offered through IBM Documentation (www.ibm.com/docs/en/zos).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com®/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS™, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those

products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., 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 (www.ibm.com/legal/copytrade.shtml).

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle, its affiliates, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

T

U

Product Number: 5650-ZOS