# Program Directory for

# IBM Z Multi-Factor Authentication

2.4.0

Program Number 5655-MA1

FMIDs HMFA240

for Use with
z/OS V2.4 or higher
z/VM V7.2 or higher

Document Date: August 2025

GI13-5220-03

**Note**

Before using this information and the product it supports, be sure to read the general information under 9.0, “Notices” on page 30.

# Contents

# Figures

# 1.0 Introduction

This program directory is intended for system programmers who are responsible for program installation and maintenance. It contains information about the material and procedures associated with the installation of IBM Z Multi-Factor Authentication. This publication refers to IBM Z Multi-Factor Authentication as IBM Z Multi-Factor Authentication.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic program materials and documentation for IBM Z Multi-Factor Authentication.
- 3.0, “Program Support” on page 6 describes the IBM support available for IBM Z Multi-Factor Authentication.
- 4.0, “Program and Service Level Information” on page 7 lists the APARs (program level) and PTFs (service level) that have been incorporated into IBM Z Multi-Factor Authentication.
- 5.0, “z/OS Installation Requirements and Considerations” on page 9 identifies the resources and considerations that are required for installing and using IBM Z Multi-Factor Authentication.
- 6.0, “z/OS Installation Instructions” on page 16 provides detailed installation instructions for IBM Z Multi-Factor Authentication. It also describes the procedures for activating the functions of IBM Z Multi-Factor Authentication, or refers to appropriate publications.
- 7.0, “z/VM Installation Requirements and Considerations” on page 26 identifies the resources and considerations that are required for installing and using IBM Z Multi-Factor Authentication with z/VM.
- 8.0, “z/VM Installation Instructions” on page 29 provides detailed installation instructions for IBM Z Multi-Factor Authentication with z/VM. It also describes the procedures for activating the functions of IBM Z Multi-Factor Authentication, or refers to appropriate publications.

Before installing IBM Z Multi-Factor Authentication, read the *CBPDO Memo To Users* and the *CBPDO Memo To Users Extension* that are supplied with this program in softcopy format and this program directory; after which, keep the documents for your reference. Section 3.2, “Preventive Service Planning” on page 6 tells you how to find any updates to the information and procedures in this program directory.

For z/OS, IBM Z Multi-Factor Authentication is supplied in a Custom-Built Product Delivery Offering (CBPDO, 5751-CS3). The program directory that is provided in softcopy format on the CBPDO is identical to the hardcopy format if one was included with your order. All service and HOLDDATA for IBM Z Multi-Factor Authentication are included on the CBPDO.

Do not use this program directory if you install IBM Z Multi-Factor Authentication with a z/OSMF Portable Software Instance (z/OSMF Portable Software Instance (ServerPac)). When you use one of those offerings, use the jobs and documentation supplied with the offering. The offering will point you to specific sections of this program directory as needed.

The IBM Z Multi-Factor Authentication support for z/VM and Linux is supplied with fix packs stored in Fix Central ( https://www.ibm.com/support/fixcentral ). Please use "IBM Z Multi-Factor Authentication" as the product to search for. Then select the MFA release you are interested in and then pick the fix pack that applies to your set up and download it.

See chapters 7.0, “z/VM Installation Requirements and Considerations” on page 26 and 8.0, “z/VM Installation Instructions” on page 29 for detailed instructions on installing MFA on a z/VM system.

## 1.1 IBM Z Multi-Factor Authentication Description

IBM Z Multi-Factor Authentication provides an alternate authentication mechanism for z/OS or z/VM that is used in conjunction with multi-factor authentication and a Security Server. This allows the z/OS Security Server RACF®, or z/VM with an approved External Security Manager such as the RACF for z/VM feature, to use multi-factor authentication mechanisms in place of the standard password or passphrase support to raise the authentication assurance level of users on their systems.

## 1.2 IBM Z Multi-Factor Authentication FMIDs

IBM Z Multi-Factor Authentication consists of the following FMIDs for z/OS:

HMFA240

# 2.0 Program Materials

An IBM program is identified by a program number. The program number for IBM Z Multi-Factor Authentication is 5655-MA1.

Basic Machine-Readable Materials are materials that are supplied under the base license and are required for the use of the product.

The program announcement material describes the features supported by IBM Z Multi-Factor Authentication. Ask your IBM representative for this information if you have not already received a copy.

## 2.1 Basic Machine-Readable Material

The distribution medium for this program is physical media or downloadable files. For z/OS, this program is in SMP/E RELFILE format and is installed by using SMP/E. See 6.0, “z/OS Installation Instructions” on page 16 for more information about how to install the program. The IBM Z Multi-Factor Authentication support for z/VM and Linux is supplied with fix packs stored in Fix Central ( https://www.ibm.com/support/fixcentral ). Please use "IBM Z Multi-Factor Authentication" as the product to search for. Then select the MFA release you are interested in and then pick the fix pack that applies to your set up and download it.

See 8.0, “z/VM Installation Instructions” on page 29 for more information about how to install the program.

You can find information about the physical media for the basic machine-readable materials for IBM Z Multi-Factor Authentication in the *CBPDO Memo To Users Extension*.

## 2.2 Program Publications

The following sections identify the basic publications for IBM Z Multi-Factor Authentication.

Figure 1 identifies the basic licensed program publications for IBM Z Multi-Factor Authentication.

*Figure 1. Basic Material: Licensed Publications*

| Publication Title | Form Number | Media Format |
|---|---|---|
| *IBM Z Multi-Factor Authentication 2.4.0 License Information* | GI13-5221-03 | Hardcopy |

Figure 2 identifies the basic unlicensed publications for IBM Z Multi-Factor Authentication. Those that are in softcopy format can be obtained from the IBM Publications Center website at https://www.ibm.com/resources/publications

*Figure 2. Basic Material: Unlicensed Publications*

| Publication Title | Direct Link |
|---|---|
| *IBM Z Multi-Factor Authentication Installation and Customization* | Please see below. |
| **Note:** https://www.ibm.com/docs/en/zma/2.4.0? topic= 24-z-multi-factor-authentication-installation- customization | |
| *IBM Z Multi-Factor Authentication User's Guide* | Please see below. |
| **Note:** https://www.ibm.com/docs/en/zma/2.4.0? topic= 24-z-multi-factor-authentication-users-guide | |

**Note:** Remove the blanks from the links in the table above before using.

**Note:** These basic unlicensed publications can be found at **IBM Products documentation** https://www.ibm.com/docs/en/products and by direct link listed in the table.

## 2.3 Program Source Materials

No program source materials or viewable program listings are provided for IBM Z Multi-Factor Authentication.

## 2.4 Publications Useful During Installation on z/OS

You might want to use the publications listed in Figure 3 during the installation of IBM Z Multi-Factor Authentication on z/OS, which can be found at **IBM Products documentation** https://www.ibm.com/docs/en/products .

*Figure 3. Publications Useful During Installation*

| Publication |
|---|
| *IBM SMP/E for z/OS User's Guide* |
| *IBM SMP/E for z/OS Reference* |
| *IBM SMP/E for z/OS Commands* |
| *IBM SMP/E for z/OS Messages, Codes, and Diagnosis* |

**Note:** IBM Publications Center https://www.ibm.com/shop/publications/order
IBM Knowledge Center https://www.ibm.com/support/knowledgecenter

## 2.5 Publications Useful During Installation on z/VM

You might want to use the publications listed in Figure 4 during the installation of IBM Z Multi-Factor Authentication on z/VM.

*Figure 4. Publications Useful During Installation*

| **Publication Title** |
|---|
| *z/VM Installation Guide* |
| *z/VM CP Planning and Administration* |
| *z/VM TCP/IP Planning and Customization* |
| *z/VM RACF Security Server Security Administrator's Guide* |
| *z/VM RACF Security Server System Programmer's Guide* |

**Note:** IBM Publications Center https://www.ibm.com/shop/publications/order
IBM Knowledge Center https://www.ibm.com/support/knowledgecenter

# 3.0 Program Support

This section describes the IBM support available for IBM Z Multi-Factor Authentication.

## 3.1 Program Services

Contact your IBM representative for specific information about available program services.

## 3.2 Preventive Service Planning

Before you install IBM Z Multi-Factor Authentication, make sure that you review the PSP bucket information for IBM Z products document https://www.ibm.com/support/pages/node/7127792. It contains the latest information concerning the installation of IBM products, including the latest service recommendations and cross-product dependencies. This information was previously available in traditional PSP buckets, which are no longer published for IBM Z products.

For support, access the Software Support Website at https://www.ibm.com/mysupport/

## 3.3 Statement of Support Procedures

Report any problems which you feel might be an error in the product materials to your IBM Support Center. You may be asked to gather and submit additional diagnostics to assist the IBM Support Center in their analysis.

Figure 5 identifies the component IDs (COMPID) for IBM Z Multi-Factor Authentication.

*Figure 5. z/OS Component IDs*

| FMID | COMPID | Component Name | RETAIN Release |
|---|---|---|---|
| HMFA240 | 565516201 | IBM Z Multi-Factor Authentication | 240 |

*Figure 6. z/VM Component IDs and Field Engineering Numbers*

| FMID or Product ID | COMPID | Component Name | FESN | RETAIN Release |
|---|---|---|---|---|
| HMFA240 | 565516201 | IBM Z Multi-Factor Authentication | 0509230 | 240 |

# 4.0 Program and Service Level Information

This section identifies the program and relevant service levels of IBM Z Multi-Factor Authentication. The program level refers to the APAR fixes that have been incorporated into the program. The service level refers to the PTFs that have been incorporated into the program.

## 4.1 Program Level Information

The following APAR fixes against previous releases of IBM Z Multi-Factor Authentication have been incorporated into this release. They are listed by FMID.

- FMID HMFA200

  PH14491
  PH15274
  PH17606
  PH18694
  PH20136
  PH20142
  PH20165
  PH20722
  PH22178
  PH23031

- FMID HMFA210

  PH25584
  PH25720
  PH26695
  PH26995
  PH27874
  PH28949
  PH29056
  PH29702
  PH29764
  PH30236
  PH30404
  PH30823
  PH30912
  PH31888
  PH32846
  PH33539
  PH36795
  PH38550
  PH39489
  PH40383
  PH41025

- FMID HMFA220

  PH38714
  PH43576
  PH43578
  PH43801
  PH44381
  PH45721
  PH48059
  PH48317
  PH48790
  PH49050
  PH55784
  PH56688

- FMID HMFA230

  TBA

## 4.2 Service Level Information

No PTFs against this release of IBM Z Multi-Factor Authentication have been incorporated into the product package.

# 5.0 z/OS Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating IBM Z Multi-Factor Authentication on z/OS. The following terminology is used:

- *Driving system*: the system on which SMP/E is executed to install the program.

  The program might have specific operating system or product level requirements for using processes, such as binder or assembly utilities during the installation.

- *Target system*: the system on which the program is configured and run.

  The program might have specific product level requirements, such as needing access to the library of another product for link-edits. These requirements, either mandatory or optional, might directly affect the element during the installation or in its basic or enhanced operation.

In many cases, you can use a system as both a driving system and a target system. However, you can make a separate IPL-able clone of the running system to use as a target system. The clone must include copies of all system libraries that SMP/E updates, copies of the SMP/E CSI data sets that describe the system libraries, and your PARMLIB and PROCLIB.

Use separate driving and target systems in the following situations:

- When you install a new level of a product that is already installed, the new level of the product will replace the old one. By installing the new level onto a separate target system, you can test the new level and keep the old one in production at the same time.
- When you install a product that shares libraries or load modules with other products, the installation can disrupt the other products. By installing the product onto a separate target system, you can assess these impacts without disrupting your production system.

## 5.1 Driving System Requirements

This section describes the environment of the driving system required to install IBM Z Multi-Factor Authentication.

### 5.1.1 Machine Requirements

The driving system can run in any hardware environment that supports the required software.

### 5.1.2 Programming Requirements

*Figure 7. Driving System Software Requirements*

| Program Number | Product Name | Minimum VRM | Minimum Service Level will satisfy these APARs | Included in the shipped product? |
|---|---|---|---|---|
| 5650-ZOS | z/OS | 02.04.00 | N/A | No |

**Note:** SMP/E is a requirement for Installation and is an element of z/OS.

**Note:** Installation might require migration to new z/OS releases to be service supported. See https://www.ibm.com/support/lifecycle/

IBM Z Multi-Factor Authentication is installed into a file system. Before installing IBM Z Multi-Factor Authentication, you must ensure that the target system file system data sets are available for processing on the driving system. OMVS must be active on the driving system and the target system file data sets must be mounted on the driving system.

zFS must be active on the driving system. Information on activating and using zFS can be found in z/OS Distributed File Service zSeries File System Administration, SC24-5989.

## 5.2 Target System Requirements

This section describes the environment of the target system required to install and use IBM Z Multi-Factor Authentication.

IBM Z Multi-Factor Authentication installs in the z/OS (Z038) SREL.

### 5.2.1 Machine Requirements

The target system can run in any hardware environment that supports the required software.

### 5.2.2 Programming Requirements

#### 5.2.2.1 Installation Requisites

Installation requisites identify products that are required and *must* be present on the system or products that are not required but *should* be present on the system for the successful installation of this product.

Mandatory installation requisites identify products that are required on the system for the successful installation of this product. These products are specified as PREs or REQs.

*Figure 8. Target System Mandatory Installation Requisites*

| Program Number | Product Name | Minimum VRM | Minimum Service Level will satisfy these APARs | Included in the shipped product? |
|---|---|---|---|---|
| Any **one** of the following: | | | | |
| 5650-ZOS | z/OS | 02.04.00 or higher | N/A | No |

**Note:** Installation might require migration to new releases to obtain support. See https://www.ibm.com/support/lifecycle/

Conditional installation requisites identify products that are *not* required for successful installation of this product but can resolve such things as certain warning messages at installation time. These products are specified as IF REQs.

IBM Z Multi-Factor Authentication has no conditional installation requisites.

### 5.2.2.2 Operational Requisites

Operational requisites are products that are required and *must* be present on the system or products that are not required but *should* be present on the system for this product to operate all or part of its functions.

Mandatory operational requisites identify products that are required for this product to operate its basic functions.

*Figure 9. Target System Mandatory Operational Requisites*

| Program Number | Product Name and Minimum VRM/Service Level |
|---|---|
| 5650-ZOS | TSO/E 02.04.00 with PTF for APAR OA58967, or higher |

**Note:** Installation might require migration to new releases to obtain support. See https://www.ibm.com/support/lifecycle/

Conditional operational requisites identify products that are *not* required for this product to operate its basic functions but are required at run time for this product to operate specific functions. These products are specified as IF REQs.

*Figure 10. Target System Conditional Operational Requisites*

| Program Number | Product Name and Minimum VRM/Service Level | Function |
|---|---|---|
| 5655-W65 | WebSphere Application Server for z/OS, component IBM HTTP Server powered by Apache 8.5.5.11 with PTF for APAR PI66183. | |
| 5655-WAS | WebSphere Application Server for z/OS, component IBM HTTP Server powered by Apache 9.0.0.2 with PTF for APAR PI66183. | |

**Note:** Installation might require migration to new releases to obtain support. See https://www.ibm.com/support/lifecycle/

### 5.2.2.3 Toleration/Coexistence Requisites

Toleration/coexistence requisites identify products that must be present on sharing systems. These systems can be other systems in a multisystem environment (not necessarily sysplex), a shared DASD environment (such as test and production), or systems that reuse the same DASD environment at different time intervals.

IBM Z Multi-Factor Authentication has no toleration/coexistence requisites.

### 5.2.2.4 Incompatibility (Negative) Requisites

Negative requisites identify products that must *not* be installed on the same system as this product.

IBM Z Multi-Factor Authentication has no negative requisites.

## 5.2.3 DASD Storage Requirements

IBM Z Multi-Factor Authentication libraries can reside on all supported DASD types.

Figure 11 lists the total space that is required for each type of library.

*Figure 11. Total DASD Space Required by IBM Z Multi-Factor Authentication*

| Library Type | Total Space Required in 3390 Trks | Description |
|---|---|---|
| Target | 525 | |
| Distribution | 1145 | |
| File System(s) | 300 | |

**Notes:**

1. For non-RECFM U data sets, IBM recommends using system-determined block sizes for efficient DASD utilization. For RECFM U data sets, IBM recommends using a block size of 32760, which is most efficient from the performance and DASD utilization perspective.
2. Abbreviations used for data set types are shown as follows.

   **U** Unique data set, allocated by this product and used by only this product. This table provides all the required information to determine the correct storage for this data set. You do not need to refer to other tables or program directories for the data set size.

   **S** Shared data set, allocated by this product and used by this product and other products. To determine the correct storage needed for this data set, add the storage size given in this table to those given in other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

   **E** Existing shared data set, used by this product and other products. This data set is *not* allocated by this product. To determine the correct storage for this data set, add the storage size given in this table to those given in other tables (perhaps in other program directories). If the data set already exists, it must have enough free space to accommodate the storage size given in this table.

   If you currently have a previous release of this product installed in these libraries, the installation of this release will delete the old release and reclaim the space that was used by the old release and any service that had been installed. You can determine whether these libraries have enough space by deleting the old release with a dummy function, compressing the libraries, and comparing the space requirements with the free space in the libraries.

   For more information about the names and sizes of the required data sets, see 6.1.8, “Allocate SMP/E Target and Distribution Libraries” on page 20.
3. Abbreviations used for the file system path type are as follows.

   **N** New path, created by this product.
   **X** Path created by this product, but might already exist from a previous release.
   **P** Previously existing path, created by another product.
4. All target and distribution libraries listed have the following attributes:
   - The default name of the data set can be changed.
   - The default block size of the data set can be changed.
   - The data set can be merged with another data set that has equivalent characteristics.
   - The data set can be either a PDS or a PDSE, with some exceptions. If the value in the "ORG" column specifies "PDS", the data set must be a PDS. If the value in "DIR Blks" column specifies "N/A", the data set must be a PDSE.
5. All target libraries listed have the following attributes:
   - These data sets can be SMS-managed, but they are not required to be SMS-managed.
   - These data sets are not required to reside on the IPL volume.
   - The values in the "Member Type" column are not necessarily the actual SMP/E element types that are identified in the SMPMCS.

6. All target libraries that are listed and contain load modules have the following attributes:
   - These data sets can not be in the LPA, with some exceptions. If the data set should be placed in the LPA, see the Special Considerations section below.
   - These data sets can be in the LNKLST. If so, see the Special Considerations section below.
   - These data sets are not required to be APF-authorized, with some exceptions. If the data set must be APF-authorized, see the Special Considerations section below.

The following figures describe the target and distribution libraries and file system paths required to install IBM Z Multi-Factor Authentication. The storage requirements of IBM Z Multi-Factor Authentication must be added to the storage required by other programs that have data in the same library or path.

**Note:** Use the data in these tables to determine which libraries can be merged into common data sets. In addition, since some ALIAS names may not be unique, ensure that no naming conflicts will be introduced before merging libraries.

*Figure 12. Storage Requirements for IBM Z Multi-Factor Authentication Target Libraries*

| Library DDNAME | Member Type | Target Volume | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|---|---|
| SAZFEXEC | Exec | TVOL | U | PDS | FB | 80 | 5 | 20 |
| SAZFLOAD | LMOD-APF | TVOL | U | PDS-E | U | 0 | 450 | N/A |
| SAZFMENU | Message | TVOL | U | PDS | FB | 80 | 5 | 20 |
| SAZFPENU | Panel | TVOL | U | PDS | FB | 80 | 15 | 20 |
| SAZFSAMP | Sample | TVOL | U | PDS | FB | 80 | 10 | 54 |
| SAZFTENU | Table | TVOL | U | PDS | FB | 80 | 5 | 20 |

*Figure 13. IBM Z Multi-Factor Authentication File System Paths*

| DDNAME | TYPE | Path Name |
|---|---|---|
| SAZFAMOD | X | /usr/lpp/IBM/azfv2r4/IBM |

*Figure 14. Storage Requirements for IBM Z Multi-Factor Authentication Distribution Libraries*

| Library DDNAME | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|
| AAZFAMOD | U | PDS | VB | 256 | 440 | 10 |
| AAZFEXEC | U | PDS | FB | 80 | 5 | 20 |
| AAZFLOAD | U | PDS-E | U | 0 | 615 | N/A |
| AAZFMENU | U | PDS | FB | 80 | 5 | 20 |
| AAZFPENU | U | PDS | FB | 80 | 15 | 20 |
| AAZFTENU | U | PDS | FB | 80 | 5 | 20 |
| AAZFSAMP | U | PDS | FB | 80 | 5 | 54 |

## 5.3 FMIDs Deleted

Installing IBM Z Multi-Factor Authentication might result in the deletion of other FMIDs. To see which FMIDs will be deleted, examine the ++VER statement in the SMPMCS of the product.

If you do not want to delete these FMIDs at this time, install IBM Z Multi-Factor Authentication into separate SMP/E target and distribution zones.

**Note:** These FMIDs are not automatically deleted from the Global Zone. If you want to delete these FMIDs from the Global Zone, use the SMP/E REJECT NOFMID DELETEFMID command. See the SMP/E Commands book for details.

## 5.4 Special Considerations

IBM Z Multi-Factor Authentication requires that the SAZFLOAD dataset be APF authorized and added to the system link list before being started.

# 6.0 z/OS Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of IBM Z Multi-Factor Authentication on z/OS.

Please note the following points:

- If you want to install IBM Z Multi-Factor Authentication into its own SMP/E environment you can use the sample jobs that are provided to define a new SMP/E CSI dataset, other datasets required for a global zone, and associated DDDEF entries.
- You can use the sample jobs that are provided to perform part or all of the installation tasks. Sample jobs exist to create the required SMP/E environment for the installation, as well as all MFA specific datasets and SMP/E definitions for the datasets.
- You can use the SMP/E dialogs instead of the sample jobs to accomplish the SMP/E installation steps, however, the supplied sample job must be used to create the required subdirectories in the target file system before performing the SMP/E APPLY.

The following installation scenarios are documented:

- Install IBM Z Multi-Factor Authentication into a standalone SMP/E environment, with a new CSI dataset that contains new global, target, and distribution zones, new SMP/E datasets, and target and distribution datasets for MFA to be installed into.
- Install IBM Z Multi-Factor Authentication into an existing SMP/E environment, with a new CSI dataset that contains target and distribution zones for IBM Z Multi-Factor Authentication, new zone specific SMP/E datasets, and new target and distribution datasets for IBM Z Multi-Factor Authentication to be installed into.
- Install IBM Z Multi-Factor Authentication into an existing SMP/E environment, using existing target and distribution zones without IBM Z Multi-Factor Authentication already installed, and new target and distribution datasets for IBM Z Multi-Factor Authentication to be installed into.
- Install IBM Z Multi-Factor Authentication into an existing SMP/E environment, using existing target and distribution zones with IBM Z Multi-Factor Authentication already installed, with existing target and distribution datasets for IBM Z Multi-Factor Authentication to be installed into. **All existing IBM Z Multi-Factor Authentication dataset and filesystem paths will remain unchanged.**

## 6.1 Installing IBM Z Multi-Factor Authentication

Please see chapters 7.0, “z/VM Installation Requirements and Considerations” on page 26 and 8.0, “z/VM Installation Instructions” on page 29 for instructions on installing MFA on a z/VM system.

### 6.1.1 SMP/E Considerations for Installing IBM Z Multi-Factor Authentication

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of IBM Z Multi-Factor Authentication.

### 6.1.2 SMP/E Options Subentry Values

The recommended values for certain SMP/E CSI subentries are shown in Figure 15. Using values lower than the recommended values can result in failures in the installation. DSSPACE is a subentry in the GLOBAL options entry. PEMAX is a subentry of the GENERAL entry in the GLOBAL options entry. See the SMP/E manuals for instructions on updating the global zone.

*Figure 15. SMP/E Options Subentry Values*

| Subentry | Value | Comment |
|---|---|---|
| DSSPACE | Existing target CSI value | IBM suggests using your existing target system CSI's DSSPACE value. |
| PEMAX | SMP/E Default | IBM recommends using the SMP/E default for PEMAX. |

### 6.1.3 SMP/E CALLLIBS Processing

IBM Z Multi-Factor Authentication does not use the CALLLIBS function provided in SMP/E.

### 6.1.4 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install IBM Z Multi-Factor Authentication:

*Figure 16 (Page 1 of 2). Sample Installation Jobs*

| Job Name | Job Type | Description | SMPTLIB Data Set |
|---|---|---|---|
| AZFJ0CSI | ALLOCATE | Sample job to allocate a new SMP/E CSI dataset - optional | 'prefix'.IBM.HMFA240.F2 |
| AZFJ1GLB | SMP/E | Sample job to allocate a new SMP/E global zone SMPPTS and create the new global zone - optional | 'prefix'.IBM.HMFA240.F2 |
| AZFJ2SMD | SMP/E | Sample job to allocate new SMP/E target/distribution zone unique datasets and create new target/distribution zones - optional | 'prefix'.IBM.HMFA240.F2 |
| AZFJ3ALO | ALLOCATE | Sample job to allocate new product target and distribution datasets - optional | 'prefix'.IBM.HMFA240.F2 |

*Figure 16 (Page 2 of 2). Sample Installation Jobs*

| Job Name | Job Type | Description | SMPTLIB Data Set |
|---|---|---|---|
| AZFJ4DDF | DDDEF | Sample job to define SMP/E DDDEF for product target and distribution datasets - optional | 'prefix'.IBM.HMFA240.F2 |
| AZFJ6MKD | MKDIR | Sample job to invoke the supplied AZFMKDIR EXEC to create target subdirectories - optional | 'prefix'.IBM.HMFA240.F2 |
| AZFJ7REC | RECEIVE | Sample RECEIVE job from pre-loaded SMPTLIB datasets | 'prefix'.IBM.HMFA240.F2 |
| AZFJ8APP | APPLY | Sample APPLY job | 'prefix'.IBM.HMFA240.F2 |
| AZFJ9ACC | ACCEPT | Sample ACCEPT job | 'prefix'.IBM.HMFA240.F2 |

The following provides a roadmap for which sample jobs should be run, depending on your needs:

*Figure 17. Sample Installation Job Roadmap*

| Environment | Jobnames |
|---|---|
| New standalone SMP/E global, target, and distribution zones, and MFA datasets | AZFJ0CSI, AZFJ1GLB, AZFJ2SMD, AZFJ3ALO, AZFJ4DDF, AZFJ5ZFS (optional, but recommended), AZFJ6MKD, AZFJ7REC, AZFJ8APP, AZFJ9ACC |
| Existing SMP/E global zone, new target and distribution zones, and MFA datasets | AZFJ0CSI, AZFJ2SMD, AZFJ3ALO, AZFJ4DDF, AZFJ5ZFS (optional, but recommended), AZFJ6MKD, AZFJ7REC, AZFJ8APP, AZFJ9ACC |
| Existing SMP/E global, target, and distribution zones, MFA not installed | AZFJ3ALO, AZFJ4DDF, AZFJ5ZFS (optional, but recommended), AZFJ6MKD, AZFJ7REC, AZFJ8APP, AZFJ9ACC |
| Existing SMP/E global, target, and distribution zones, MFA installed | AZFJ6MKD, AZFJ7REC, AZFJ8APP, AZFJ9ACC |

If you are using an existing SMP/E global zone, you can access the sample installation jobs by performing an SMP/E RECEIVE (refer to 6.1.12, “Perform SMP/E RECEIVE” on page 22) and then copy the sample jobs from the SMPTLIB dataset 'prefix'.IBM.HMFA240.F2 to a work dataset for editing and submission.

The sample JCL expects the work dataset to be named 'AZF.INSTALL'. If a different name is used then the JCLLIB statement in each of the sample jobs must be edited before being submitted.

You can also copy the sample installation jobs from the product files by submitting the following job. Before you submit the job, add a job card and change the lowercase parameters to uppercase values to meet the requirements of your site.

```
//STEP1    EXEC PGM=IEBCOPY
//SYSPRINT DD SYSOUT=*
//SYSUT1   DD DSN=IBM.fmid.F2,UNIT=SYSALLDA,DISP=SHR,
//         VOL=SER=filevol
//SYSUT2   DD DSNAME=work-dataset,
//         DISP=(NEW,CATLG,DELETE),
//         VOL=SER=dasdvol,UNIT=SYSALLDA,
//         SPACE=(TRK,(primary,secondary,dir))
//SYSUT3   DD UNIT=SYSALLDA,SPACE=(CYL,(1,1))
//SYSIN    DD DUMMY*
```

See the following information to update the statements in the previous sample:

SYSUT1:

**filevol** is the volume serial of the DASD device where the downloaded files reside.

SYSUT2:

**work-dataset** is the name of the output data set where the sample jobs are copied.

The sample JCL expects the work dataset to be named 'AZF.INSTALL'. If a different name is used then the JCLLIB statement in each of the sample jobs must be edited before being submitted.
**dasdvol** is the volume serial of the DASD device where the output data set resides. The VOL=SER= specification may be omitted if an appropriate SMS policy exists.

Prior to submitting the sample jobs you need to edit member AZFIOPTS in the work dataset and make any installation required changes to it. Any SET value containing "<...>" needs to be replaced with an appropriate installation value, such as in the statements-

```
// SET IMCS=<prefix>.SMPMCS
// SET ITLPFX='RFPREFIX(<prefix>)'
```

The value "<prefix>" might be replaced with a value such as "SMPE.INSTALL" in the two SET statements.

### 6.1.5 Define a new SMP/E CSI dataset

Run this job if you want to create a new SMP/E global zone for IBM Z Multi-Factor Authentication, or to create new SMP/E target and distribution zones for IBM Z Multi-Factor Authentication.

Edit and submit sample job AZFJ0CSI to define an SMP/E CSI dataset for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly..*

### 6.1.6 Create an SMP/E Global zone

Run this job if you want to create new SMP/E global zone just for IBM Z Multi-Factor Authentication.

Edit and submit sample job AZFJ1GLB to create the SMP/E global zone, and any zone specific SMP/E libraries for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly..*

### 6.1.7 Create SMP/E Target and Distribution zones

Run this job if you want to create new SMP/E target and distribution zones to install IBM Z Multi-Factor Authentication into.

Edit and submit sample job AZFJ2SMD to create the SMP/E target and distribution zones, and any zone specific SMP/E libraries for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly..*

### 6.1.8 Allocate SMP/E Target and Distribution Libraries

Run this job if you have created new SMP/E target and distribution zones to install IBM Z Multi-Factor Authentication into.

Edit and submit sample job AZFJ3ALO to allocate the SMP/E target and distribution libraries for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly.

### 6.1.9 Create SMP/E Target and Distribution zone DDDEFs

Run this job if you want to create new DDDEF entries in existing target and distribution zones, or you have created new SMP/E target and distribution zones to install IBM Z Multi-Factor Authentication into.

Edit and submit sample job AZFJ4DDF to create DDDEF entries for the SMP/E target and distribution libraries for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly.

## 6.1.10 Allocate, create and mount ZFS Files (Optional)

Run this job to create a new zFS filesystem dataset for IBM Z Multi-Factor Authentication.

If you plan to install IBM Z Multi-Factor Authentication into a new z/OS UNIX file system, you can edit and submit the optional AZFJ5ZFS job to perform the following tasks:

- Create the z/OS UNIX filesystem dataset
- Create a mountpoint
- Mount the z/OS UNIX filesystem on the mountpoint

Consult the instructions in the sample job for more information.

The required z/OS UNIX file system type is *zFS*. The recommended mountpoint is */usr/lpp/IBM/azfv2r4*.

Before running the sample job to create the z/OS UNIX file system, you must ensure that OMVS is active on the driving system. zFS must be active on the driving system if you are installing IBM Z Multi-Factor Authentication into a file system that is zFS.

If you create a new file system for this product, consider updating the BPXPRMxx PARMLIB member to mount the new file system at IPL time. This action can be helpful if an IPL occurs before the installation is completed.

```
MOUNT FILESYSTEM('#dsn')

MOUNTPOINT('/usr/lpp/IBM/azfv2r4')

MODE(RDWR)        /* can be MODE(READ) */
TYPE(ZFS) PARM('AGGRGROW') /* zFS, with extents */
```

See the following information to update the statements in the previous sample:

**#dsn** is the name of the data set holding the z/OS UNIX file system.
**/usr/lpp/IBM/azfv2r4** is the name of the mountpoint where the z/OS UNIX file system will be mounted.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly.

## 6.1.11 Allocate File System Paths

Run this job to create all MFA required paths where IBM Z Multi-Factor Authentication files are to be installed.

This job must be run even if IBM Z Multi-Factor Authentication was previously installed so that any new paths will be created prior to performing the SMP/E APPLY.

The target file system data set must be mounted on the driving system when running the sample AZFJ6MKD job since the job will create paths in the file system.

Before running the sample job to create the paths in the file system, you must ensure that OMVS is active on the driving system and that the target system's zFS file system is mounted to the driving system. zFS must be active on the driving system.

If you plan to install IBM Z Multi-Factor Authentication into a new zFS file system, you must create the mountpoint and mount the new file system to the driving system for IBM Z Multi-Factor Authentication.

The recommended mountpoint is */usr/lpp/IBM/azfv2r4*.

Edit and submit sample job AZFJ6MKD to allocate the zFS paths for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

If you create a new file system for this product, consider updating the BPXPRMxx PARMLIB member to mount the new file system at IPL time. This action can be helpful if an IPL occurs before the installation is completed.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly.

## 6.1.12 Perform SMP/E RECEIVE

If you have obtained IBM Z Multi-Factor Authentication as part of a CBPDO, use the RCVPDO job in the CBPDO RIMLIB data set to receive the IBM Z Multi-Factor Authentication FMIDs, service, and HOLDDATA that are included on the CBPDO package. For more information, see the documentation that is included in the CBPDO.

You can also choose to edit and submit sample job AZFJ7REC to perform the SMP/E RECEIVE for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** You will receive a return code of 0 if this job runs correctly.

## 6.1.13 Perform SMP/E APPLY

1. Ensure that you have the latest HOLDDATA; then edit and submit sample job AZFJ8APP to perform an SMP/E APPLY CHECK for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

   The latest HOLDDATA is available through several different portals, including https://public.dhe.ibm.com/s390/assigns/ or https://www.ibm.com/support/pages/enhanced-holddata-zos for usage instructions. The latest HOLDDATA may identify HIPER and FIXCAT APARs for the FMIDs you will be installing. An APPLY CHECK will help you determine if any HIPER or FIXCAT APARs are applicable to the FMIDs you are installing. If there are any applicable HIPER or FIXCAT APARs, the APPLY CHECK will also identify fixing PTFs that will resolve the APARs, if a fixing PTF is available.

   You should install the FMIDs regardless of the status of unresolved HIPER or FIXCAT APARs. However, do not deploy the software until the unresolved HIPER and FIXCAT APARs have been analyzed to determine their applicability. That is, before deploying the software either ensure fixing

PTFs are applied to resolve all HIPER or FIXCAT APARs, or ensure the problems reported by all HIPER or FIXCAT APARs are not applicable to your environment.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the PRE, ID, REQ, and IFREQ on the APPLY CHECK. The SMP/E root cause analysis identifies the cause only of *errors* and not of *warnings* (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings, instead of errors).

Here are sample APPLY commands:

a. To ensure that all recommended and critical service is installed with the FMIDs, receive the latest HOLDDATA and use the APPLY CHECK command as follows

   ```
   APPLY S(fmid,fmid,...) CHECK
   FORFMID(fmid,fmid,...)
   SOURCEID(RSU*)
   FIXCAT(IBM.ProductInstall-RequiredService)
   GROUPEXTEND .
   ```

   Some HIPER APARs might not have fixing PTFs available yet. You should analyze the symptom flags for the unresolved HIPER APARs to determine if the reported problem is applicable to your environment and if you should bypass the specific ERROR HOLDs in order to continue the installation of the FMIDs.

   This method requires more initial research, but can provide resolution for all HIPERs that have fixing PTFs available and are not in a PE chain. Unresolved PEs or HIPERs might still exist and require the use of BYPASS.

b. To install the FMIDs without regard for unresolved HIPER APARs, you can add the BYPASS(HOLDCLASS(HIPER)) operand to the APPLY CHECK command. This will allow you to install FMIDs even though one or more unresolved HIPER APARs exist. After the FMIDs are installed, use the SMP/E REPORT ERRSYSMODS command to identify unresolved HIPER APARs and any fixing PTFs.

   ```
   APPLY S(fmid,fmid,...) CHECK
   FORFMID(fmid,fmid,...)
   SOURCEID(RSU*)
   FIXCAT(IBM.ProductInstall-RequiredService)
   GROUPEXTEND
   BYPASS(HOLDCLASS(HIPER)) .
    ..any other parameters documented in the program directory
   ```

   This method is quicker, but requires subsequent review of the Exception SYSMOD report produced by the REPORT ERRSYSMODS command to investigate any unresolved HIPERs. If you have received the latest HOLDDATA, you can also choose to use the REPORT MISSINGFIX command and specify Fix Category IBM.PRODUCTINSTALL-REQUIREDSERVICE to investigate missing recommended service.

   If you bypass HOLDs during the installation of the FMIDs because fixing PTFs are not yet available, you can be notified when the fixing PTFs are available by using the APAR Status Tracking (AST) function of ServiceLink or the APAR Tracking function of ResourceLink.

2. After you take actions that are indicated by the APPLY CHECK, remove the CHECK operand and run the job again to perform the APPLY.

   **Note:** The GROUPEXTEND operand indicates that SMP/E applies all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

   **Expected Return Codes and Messages from APPLY CHECK:** You will receive a return code of 0 if this job runs correctly.

   **Expected Return Codes and Messages from APPLY:** You will receive a return code of 0 if this job runs correctly.

### 6.1.14 Perform SMP/E ACCEPT

Edit and submit sample job AZFJ9ACC to perform an SMP/E ACCEPT CHECK for IBM Z Multi-Factor Authentication. Consult the instructions in the sample job for more information.

To receive the full benefit of the SMP/E Causer SYSMOD Summary Report, do *not* bypass the PRE, ID, REQ, and IFREQ on the ACCEPT CHECK. The SMP/E root cause analysis identifies the cause of *errors* but not *warnings* (SMP/E treats bypassed PRE, ID, REQ, and IFREQ conditions as warnings rather than errors).

Before you use SMP/E to load new distribution libraries, it is recommended that you set the ACCJCLIN indicator in the distribution zone. In this way, you can save the entries that are produced from JCLIN in the distribution zone whenever a SYSMOD that contains inline JCLIN is accepted. For more information about the ACCJCLIN indicator, see the description of inline JCLIN in the SMP/E Commands book for details.

After you take actions that are indicated by the ACCEPT CHECK, remove the CHECK operand and run the job again to perform the ACCEPT.

**Note:** The GROUPEXTEND operand indicates that SMP/E accepts all requisite SYSMODs. The requisite SYSMODS might be applicable to other functions.

**Expected Return Codes and Messages from ACCEPT CHECK:** You will receive a return code of 0 if this job runs correctly.

If PTFs that contain replacement modules are accepted, SMP/E ACCEPT processing will link-edit or bind the modules into the distribution libraries. During this processing, the Linkage Editor or Binder might issue messages that indicate unresolved external references, which will result in a return code of 4 during the ACCEPT phase. You can ignore these messages, because the distribution libraries are not executable and the unresolved external references do not affect the executable system libraries.

**Expected Return Codes and Messages from ACCEPT:** You will receive a return code of 0 if this job runs correctly.

### 6.1.15 Run REPORT CROSSZONE

The SMP/E REPORT CROSSZONE command identifies requisites for products that are installed in separate zones. This command also creates APPLY and ACCEPT commands in the SMPPUNCH data set. You can use the APPLY and ACCEPT commands to install those cross-zone requisites that the SMP/E REPORT CROSSZONE command identifies.

After you install IBM Z Multi-Factor Authentication, it is recommended that you run REPORT CROSSZONE against the new or updated target and distribution zones. REPORT CROSSZONE requires a global zone with ZONEINDEX entries that describe all the target and distribution libraries to be reported on.

For more information about REPORT CROSSZONE, see the SMP/E manuals.

### 6.1.16 Cleaning Up Obsolete Data Sets, Paths, and DDDEFs

There are no datasets to remove after the installation.

The following file system paths, which were created and used by previous releases of this product, are no longer used in this release. You can delete these obsolete file system paths after you delete the previous release from your system.

- /usr/lpp/IBM/azfv1r3
- /usr/lpp/IBM/azfv2r0
- /usr/lpp/IBM/azfv2r1
- /usr/lpp/IBM/azfv2r2
- /usr/lpp/IBM/azfv2r3

There are no DDDEFs to clean up after the installation.

## 6.2 Activating IBM Z Multi-Factor Authentication

### 6.2.1 File System Execution

If you mount the file system in which you have installed IBM Z Multi-Factor Authentication in read-only mode during execution, then you do not have to take further actions to activate IBM Z Multi-Factor Authentication.

## 6.3 Product Customization

The publication *IBM Z Multi-Factor Authentication Installation and Customization* (SC27-8447) contains the necessary information to customize and use IBM Z Multi-Factor Authentication.

# 7.0 z/VM Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating IBM Z Multi-Factor Authentication on z/VM. The following terminology is used:

- *Target system*: the system on which the program is configured and run.

## 7.1 z/VM Target System Requirements

This section describes the environment of the z/VM target system required to install and use IBM Z Multi-Factor Authentication.

## 7.1.1 z/VM Machine Requirements

The target system can run in any hardware environment that supports the required software.

## 7.1.2 Programming Requirements

### 7.1.2.1 z/VM Installation Requisites

IBM Z Multi-Factor Authentication has no mandatory installation requisites for z/VM installation.

IBM Z Multi-Factor Authentication has no conditional installation requisites for z/VM installation.

### 7.1.2.2 z/VM Operational Requisites

z/VM operational requisites are products that are required and *must* be present on the system or products that are not required but *should* be present on the system for this product to operate all or part of its functions.

Mandatory operational requisites identify products that are required for this product to operate its basic functions.

*Figure 18. z/VM Target System Mandatory Operational Requisites*

| Program Number | Product Name and Minimum VRM/Service Level |
|---|---|
| 5741-A09 | z/VM 7.2.0 and either<br>• SUSE Linux Enterprise Server for IBM Z and LinuxONE, release 15 or later<br>• RedHat Enterprise Linux for IBM Z and LinuxONE, release 9.x or later |

For the z/VM system, an External Security Manager must be installed in order for IBM Z Multi-Factor Authentication to operate in any fashion. If using the IBM z/VM RACF Security Server feature, the system must include the PTF for APAR VM66367. Please consult relevant documentation if using any other External Security Manager product.

The following rpms for your Linux Distribution must be installed:

- SUSE Linux Enterprise Server for IBM Z and LinuxONE
  - postgresql13-server or later
  - libpq5
  - openCryptoki
  - openCryptoki-64bit
  - OpenSSL 3.0 or later
- RedHat Enterprise Linux for IBM Z and LinuxONE
  - postgresql-server 13.x or later
  - openCryptoki
  - openCryptoki-swtok
  - OpenSSL 3.0 or later

Conditional operational requisites identify products that are *not* required for this product to operate its basic functions but are required at run time for this product to operate specific functions.

IBM Z Multi-Factor Authentication has no conditional operational requisites.

#### 7.1.2.3 z/VM Toleration/Coexistence Requisites

Toleration/coexistence requisites identify products that must be present on sharing systems. These systems can be other systems in a multisystem environment (not necessarily a Single System Image cluster), a shared DASD environment (such as test and production), or systems that reuse the same DASD environment at different time intervals.

IBM Z Multi-Factor Authentication has no toleration/coexistence requisites.

#### 7.1.2.4 z/VM Incompatibility (Negative) Requisites

Negative requisites identify products that must *not* be installed on the same system as this product.

IBM Z Multi-Factor Authentication has no negative requisites.

### 7.1.3 z/VM DASD Storage Requirements

The MFA server runs on a Linux on IBM Z image and there are no additional DASD requirements on the z/VM systems beyond those required for the Linux system.

#### 7.1.3.1 z/VM Storage Requirements for IBM Z Multi-Factor Authentication Target Libraries

**Note:** z/VM does not require pre–allocation of files. Just provide enough room on the disks where the operational files will be copied.

# 8.0 z/VM Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of IBM Z Multi-Factor Authentication on z/VM.

## 8.1 Installing IBM Z Multi-Factor Authentication on z/VM

### 8.1.1 MFA Distribution

The IBM Z Multi-Factor Authentication support for z/VM and Linux is shipped as fix packs stored in Fix Central ( https://www.ibm.com/support/fixcentral ). Please use "IBM Z Multi-Factor Authentication" as the product to search for. Then select the MFA release you are interested in and then pick the fix pack that applies to your set up and download it.

You should select the rpm or pam file for your distribution and install MFA as documented in

- *IBM Z Multi-Factor Authentication for z/VM*, Document number SC27-4938.

## 8.2 Activating IBM Z Multi-Factor Authentication on z/VM

The steps for customization are found in the documentation for *IBM Z Multi-Factor Authentication for z/VM*, Document number SC27-4938.

## 9.0 Notices

This information was developed for products and services offered in the U.S.A. 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.

APAR numbers are provided in this document to assist in locating PTFs that may be required. Ongoing problem reporting may result in additional APARs being created. Therefore, the APAR lists in this document may not be complete. To obtain current service recommendations and to identify current product service requirements, always refer to the instructions in the **Service Recommendation Summary and Service Recommendations** and **Cross Product Dependencies** sections of the **PSP bucket information for IBM Z products** at https://www.ibm.com/support/pages/node/7127792, to ensure you have all required service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, New York 10504-1785
USA

For license inquiries regarding double-byte (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

## 9.1 Trademarks

IBM, the IBM logo, and other IBM trademark listed on the IBM Trademarks List are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

# Reader's Comments

**Program Directory for IBM Z Multi-Factor Authentication, August 2025** We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Send your comments by emailing us at ibmdocs@us.ibm.com, and include the following information:

```
Your name and address
Your email address
Your telephone or fax number
The publication title and order number
The topic and page number related to your comment
The text of your comment
```

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

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

Thank you for your participation.

IBM

Printed in Ireland

GI13-5220-03