# Program Directory for

# IBM Security zSecure Compliance and Auditing

V2.3.0

Program Number 5655-N24

for Use with
z/OS

Document Date: August 2017

GI13-2294-06

**Note**

Before using this information and the product it supports, be sure to read the general information under 7.0, “Notices” on page 25.

# Contents

**Release information** . . . . . iv

**1.0 Introduction** . . . . . 1
1.1 IBM Security zSecure Compliance and Auditing Description . . . . . 1
1.2 IBM Security zSecure Compliance and Auditing FMIDs . . . . . 2

**2.0 Program Materials** . . . . . 3
2.1 Basic Machine-Readable Material . . . . . 3
2.2 Optional Machine-Readable Material . . . . . 3
2.3 Program Publications . . . . . 3
2.4 Program Source Materials . . . . . 4
2.5 Publications Useful During Installation . . . . . 5

**3.0 Program Support** . . . . . 6
3.1 Program Services . . . . . 6
3.2 Preventive Service Planning . . . . . 6
3.3 Statement of Support Procedures . . . . . 7

**4.0 Program and Service Level Information** . . . . . 8
4.1 Program Level Information . . . . . 8
4.2 Service Level Information . . . . . 8

**5.0 Installation Requirements and Considerations** . . . . . 9
5.1 Driving System Requirements . . . . . 9
5.1.1 Machine Requirements . . . . . 9
5.1.2 Programming Requirements . . . . . 9
5.2 Target System Requirements . . . . . 10
5.2.1 Machine Requirements . . . . . 10
5.2.2 Programming Requirements . . . . . 10
5.2.2.1 Installation Requisites . . . . . 10
5.2.2.2 Operational Requisites . . . . . 11
5.2.2.3 Toleration/Coexistence Requisites . . . . . 11
5.2.2.4 Incompatibility (Negative) Requisites . . . . . 11
5.2.3 DASD Storage Requirements . . . . . 11
5.3 FMIDs Deleted . . . . . 15
5.4 Special Considerations . . . . . 15

**6.0 Installation Instructions** . . . . . 16
6.1 Installing zSecure . . . . . 16
6.1.1 SMP/E Considerations for Installing zSecure . . . . . 16
6.1.2 SMP/E Options Subentry Values . . . . . 16
6.1.3 Sample Jobs . . . . . 17

6.1.4 Batch-mode Updating the jobs (optional) . . . 18
6.1.5 Setup SMP/E CSI and Zones (optional) . . . 19
6.1.5.1 Allocate SMP/E GLOBAL CSI (Optional) . . . 19
6.1.5.2 Allocate SMP/E Target/DLIB CSI (Optional) . . . 19
6.1.5.3 Define OPTIONS entry to SMP/E GLOBAL/Target/DLIB CSI (Optional) . . . 19
6.1.6 Perform SMP/E RECEIVE . . . 19
6.1.7 Allocate SMP/E Target and Distribution Libraries . . . 20
6.1.8 Create DDDEF Entries . . . 20
6.1.9 Perform SMP/E APPLY . . . 20
6.1.10 Perform SMP/E ACCEPT . . . 22
6.1.11 Run REPORT CROSSZONE . . . 23
6.2 Activating zSecure . . . 23
6.2.1 Post install . . . 23

**7.0 Notices** . . . 25
7.1 Trademarks . . . 26

**Contacting IBM Software Support** . . . 27

# Figures

1. Basic Material: Licensed Publications . . . 4
2. Basic Material: Unlicensed . . . 4
3. Publications Useful During Installation . . . 5
4. PSP Upgrade and Subset ID . . . 6
5. Component IDs . . . 7
6. Driving System Software Requirements . . . 10
7. Target System Mandatory Installation Requisites . . . 10
8. Target System Mandatory Operational Requisites for all zSecure products . . . 11
9. Total DASD Space Required by zSecure . . . 12
10. Storage Requirements for zSecure Target Libraries . . . 13
11. Storage Requirements for zSecure Distribution Libraries . . . 14
12. Storage Requirements for zSecure Non-SMP/E Data Sets . . . 14
13. SMP/E Options Subentry Values . . . 17
14. Sample Installation Jobs . . . 17

# Release information

IBM Security zSecure Compliance and Auditing is functionally equivalent to the following IBM Security products:

- Security zSecure Audit for RACF
- Security zSecure Audit for Top Secret
- Security zSecure Audit for ACF2
- Security zSecure Alert for ACF2
- Security zSecure Alert for RACF
- Security zSecure Command Verifier

The Security zSecure Release Information topics include details on new features and enhancements, incompatibility warnings, and documentation update information for your Security zSecure product. You can review the most current version of the release information from the following links:

- What's new: New feature and enhancements in zSecure 2.3.0.
  http://www.ibm.com/support/knowledgecenter/SS2RWS_2.3.0/com.ibm.zsecure.doc_2.3.0/about_this_release/about_rel_whats_new.html
- Release notes: Information you need before installing zSecure 2.3.0, such as system requirements, incompatibility warnings, and known problems.
  http://www.ibm.com/support/knowledgecenter/SS2RWS_2.3.0/com.ibm.zsecure.doc_2.3.0/about_this_release/releaseinfo_relnotes.html

# 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 Security zSecure Compliance and Auditing. This publication refers to IBM Security zSecure Compliance and Auditing as zSecure.

The Program Directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic program materials and documentation for zSecure.
- 3.0, “Program Support” on page 6 describes the IBM support available for zSecure.
- 4.0, “Program and Service Level Information” on page 8 lists the APARs (program level) and PTFs (service level) that have been incorporated into zSecure.
- 5.0, “Installation Requirements and Considerations” on page 9 identifies the resources and considerations that are required for installing and using zSecure.
- 6.0, “Installation Instructions” on page 16 provides detailed installation instructions for zSecure. It also describes the procedures for activating the functions of zSecure, or refers to appropriate publications.

Before installing zSecure, 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; then keep them for future 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.

zSecure is supplied in a Custom-Built Product Delivery Offering (CBPDO, 5751-CS3). The program directory that is provided in softcopy format on the CBPDO tape is identical to the hardcopy format if one was included with your order. All service and HOLDDATA for zSecure are included on the CBPDO tape.

Do not use this program directory if you install zSecure with a SystemPac or 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.

## 1.1 IBM Security zSecure Compliance and Auditing Description

IBM Security zSecure Command Verifier compares RACF commands entered by any means against defined security policy and adapts or blocks noncompliant ones. More detailed information and installation instructions for the Command Verifier component are available in publication number GI13-2284 "Program Directory for IBM Security zSecure Command Verifier" which is distributed with the IBM Security zSecure Compliance and Auditing materials.

IBM Security zSecure Audit looks across your various mainframe systems, measuring and auditing status and events. The technology provides standard and customized reports that warn of policy exceptions or

violations that indicate a security breach or weakness. IBM Security zSecure Audit is available for RACF, ACF2, and Top Secret.

IBM Security zSecure Audit ships with a component of the IBM Common Data Provider product called the System Data Engine. This component is designed to assist in sharing SMF and other information between products to meet common data needs. If you want to use this component for your QRadar SIEM near real-time feed, you must install FMID HHBO11E. Please see the related PDIR for the installation process for SDE, GI13-4177.

IBM Security zSecure Alert is a real-time monitor for z/OS systems protected with RACF or ACF2 that issues alerts for important events relevant for the security of the system at the time they occur.

## 1.2 IBM Security zSecure Compliance and Auditing FMIDs

IBM Security zSecure Compliance and Auditing consists of the following FMIDs:

| **Product/Feature** | **FMID(s)** |
|---|---|
| zSecure Audit for RACF | HCKR230, HC4R230, JCKA23R |
| zSecure Audit for ACF2 | HCKR230, HC4R230, JC2A230, JC2A23A |
| zSecure Audit for Top Secret | HCKR230, HC4R230, JCKT23T |
| zSecure Alert for RACF | HCKR230, HC4R230, JC2P23R |
| zSecure Alert for ACF2 | HCKR230, HC4R230, JC2A230, JC2P23A |
| zSecure Command Verifier | JC4R230, HC4R230 |

# 2.0 Program Materials

An IBM program is identified by a program number.
The program number for IBM Security zSecure Compliance and Auditing is 5655-N24.

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 zSecure. 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.

| Program Number | Product | Feature Number | Type | Volume | Tape VOLSER |
|---|---|---|---|---|---|
| 5655-N24 | IBM Security zSecure Compliance and Auditing | N/A | CBPDO | N/A | See CBPDO memo |

5655-N24 is functionally equivalent to 5655-N17 (IBM Security zSecure Audit), 5655-N19 (IBM Security zSecure Command Verifier), and 5655-N21 (IBM Security zSecure Alert).

It is installed using SMP/E, and is in SMP/E RELFILE format. See 6.0, “Installation Instructions” on page 16 for more information about how to install the program.

You can find information about the physical media for the basic machine-readable materials for zSecure in the *CBPDO Memo To Users Extension*.

## 2.2 Optional Machine-Readable Material

No optional machine-readable materials are provided for zSecure.

## 2.3 Program Publications

The following sections identify the basic publications for zSecure.

Figure 1 identifies the basic licensed program publications for zSecure.

*Figure 1. Basic Material: Licensed Publications*

| Publication Title | Form Number |
|---|---|
| IBM Security zSecure Admin and Audit for RACF User Reference Manual 2.3.0 | LC27-5639 |
| IBM Security zSecure Audit for ACF2 User Reference Manual 2.3.0 | LC27-5640 |
| IBM Security zSecure Audit for Top Secret User Reference Manual Version 2.3.0 | LC27-5641 |
| IBM Security zSecure CARLa Command Reference 2.3.0 | LC27-6533 |

These licensed publications are provided on the IBM Security zSecure Documentation CD (LCD7-5373). To download the .iso file for this Documentation CD, see the instructions for Downloading Documentation that are included with the product materials. If you do not have access to this information, see zSecure documentation on the IBM Knowledge Center for IBM Security zSecure Suite 2.3.0
http://www.ibm.com/support/knowledgecenter/SS2RWS_2.3.0/com.ibm.zsecure.doc_2.3.0/DITA_shared_files/publications.html

Figure 2 identifies the basic unlicensed publications for zSecure. Those that are in softcopy format publications can be obtained from the IBM Publications Center website at http://www.ibm.com/shop/publications/order/.

*Figure 2. Basic Material: Unlicensed*

| Publication Title | Form Number |
|---|---|
| IBM Security zSecure Suite: CARLa driven components, Installation and Deployment Guide Version 2.3.0 | SC27-5638 |
| IBM Security zSecure Alert User Reference Manual Version 2.3.0 | SC27-5642 |
| IBM Security zSecure Audit for ACF2 Getting Started Guide Version 2.3.0 | GI13-2325 |
| IBM Security zSecure Suite: Admin and Audit for RACF Getting Started Guide Version 2.3.0 | GI13-2324 |
| IBM Security zSecure Admin and Audit for RACF line commands and primary commands summary Version 2.3.0 | SC27-6581 |
| IBM Security zSecure Command Verifier User Guide 2.3.0 | SC27-5648 |
| IBM Security zSecure Suite: Messages Guide Version 2.3.0 | SC27-5643 |

No optional publications are provided for zSecure.

## 2.4 Program Source Materials

No program source materials or viewable program listings are provided for zSecure.

## 2.5 Publications Useful During Installation

You might want to use the publications listed in Figure 3 on page 5 during the installation of zSecure.

*Figure 3. Publications Useful During Installation*

| Publication Title | Form Number |
|---|---|
| *IBM SMP/E for z/OS User's Guide* | SA23-2277 |
| *IBM SMP/E for z/OS Commands* | SA23-2275 |
| *IBM SMP/E for z/OS Reference* | SA23-2276 |
| *IBM SMP/E for z/OS Messages, Codes, and Diagnosis* | GA32-0883 |

# 3.0 Program Support

This section describes the IBM support available for zSecure.

## 3.1 Program Services

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

## 3.2 Preventive Service Planning

Before you install zSecure, make sure that you have reviewed the current Preventive Service Planning (PSP) information. Review the PSP Bucket for General Information, Installation Documentation, and the Cross Product Dependencies sections. For the Recommended Service section, instead of reviewing the PSP Bucket, it is recommended you use the IBM.ProductInstall-RequiredService fix category in SMP/E to ensure you have all the recommended service installed. Use the **FIXCAT(IBM.ProductInstall-RequiredService)** operand on the **APPLY CHECK command**. See 6.1.9, “Perform SMP/E APPLY” on page 20 for a sample APPLY command

If you obtained zSecure as part of a CBPDO, HOLDDATA is included.

If the CBPDO for zSecure is older than two weeks by the time you install the product materials, you can obtain the latest PSP Bucket information by going to the following website:

http://www14.software.ibm.com/webapp/set2/psearch/search?domain=psp

You can also use S/390 SoftwareXcel or contact the IBM Support Center to obtain the latest PSP Bucket information.

For program support, access the Software Support Website at http://www.ibm.com/software/support/.

PSP Buckets are identified by UPGRADEs, which specify product levels; and SUBSETs, which specify the FMIDs for a product level. The UPGRADE and SUBSET values for zSecure are included in Figure 4.

*Figure 4 (Page 1 of 2). PSP Upgrade and Subset ID*

| UPGRADE | SUBSET | Description |
|---|---|---|
| SECZSCADM230 | HCKR230 | Security zSecure Base |
| SECZSCADM230 | HC4R230 | Security zSecure Command Verifier base |
| SECZSCAUD230 | JCKA23R | Security zSecure Audit for RACF |
| SECZSCAUD230 | JCKT23T | Security zSecure Audit for Top Secret |
| SECZSCAUD230 | JC2A23A | Security zSecure Audit for ACF2 |

*Figure 4 (Page 2 of 2). PSP Upgrade and Subset ID*

| UPGRADE | SUBSET | Description |
|---|---|---|
| SECZSCAUD230 | JC2A230 | Security zSecure Audit for ACF2 Base |
| SECZSCALT230 | JC2P23A | Security zSecure Alert for ACF2 |
| SECZSCALT230 | JC2P23R | Security zSecure Alert for RACF |
| SECZSCCMD230 | JC4R230 | Security zSecure Command Verifier Policy |

## 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 zSecure.

*Figure 5. Component IDs*

| FMID | COMPID | Component Name | RETAIN Release |
|---|---|---|---|
| HCKR230 | 5655T0100 | Security zSecure Base | 230 |
| HC4R230 | 5655T0100 | Security zSecure Command Verifier base | 230 |
| JCKA23R | 5655T0200 | Security zSecure Audit for RACF | 23R |
| JCKT23T | 5655T0200 | Security zSecure Audit for Top Secret | 23T |
| JC2A23A | 5655T0200 | Security zSecure Audit for ACF2 | 23A |
| JC2A230 | 5655T0200 | Security zSecure Audit for ACF2 Base | 230 |
| JC2P23A | 5655T1100 | Security zSecure Alert for ACF2 | 23A |
| JC2P23R | 5655T1100 | Security zSecure Alert for RACF | 23R |
| JC4R230 | 5655T07CV | Security zSecure Command Verifier Policy | 230 |

# 4.0 Program and Service Level Information

This section identifies the program and relevant service levels of zSecure. 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

No APARs have been incorporated into zSecure.

## 4.2 Service Level Information

No PTFs against this release of zSecure have been incorporated into the product package.

Frequently check the zSecure PSP Bucket for HIPER and SPECIAL attention PTFs against all FMIDs that you must install. You can also receive the latest HOLDDATA, then add the **FIXCAT(IBM.PRODUCTINSTALL-REQUIREDSERVICE)** operand on your APPLY CHECK command. This will allow you to review the recommended and critical service that should be installed with your FMIDs.

# 5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating zSecure. 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 zSecure.

### 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 6. Driving System Software Requirements*

| 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 | V02.01.00 or later | N/A | No |

## 5.2 Target System Requirements

This section describes the environment of the target system required to install and use zSecure.

zSecure 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 7. Target System Mandatory Installation Requisites*

| Program Number | Product Name | Minimum VRM | Minimum Service Level will satisfy these APARs | Included in the shipped product? |
|---|---|---|---|---|
| 5650-ZOS | z/OS | V02.01.00 later | N/A | No |

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.

zSecure 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. These products are specified as PREs or REQs.

*Figure 8. Target System Mandatory Operational Requisites for all zSecure products*

| Program Number | Product Name and Minimum VRM/Service Level |
|---|---|
| 5650-ZOS | z/OS Version 2.1.0 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. These products are specified as IF REQs.

zSecure has no conditional operational requisites.

### 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.

zSecure 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.

zSecure has no negative requisites.

## 5.2.3 DASD Storage Requirements

zSecure libraries can reside on all supported DASD types.

Figure 9 lists the total space that is required for each type of library.

*Figure 9. Total DASD Space Required by zSecure*

| Library Type | Total Space Required in 3390 Trks |
|---|---|
| Target | 3446 |
| Distribution | 3525 |

**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 6.1.7, “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.

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 be in the LPALIST, but they are not required to be in the LPALIST.
   - Loadmodules from these data sets cannot be added to the active LPA using Dynamic LPA Services (CSVDYLPA or SETPROG LPA).
   - These data sets can be in the LNKLIST.
   - These data sets must be APF-authorized.

The following figures describe the target and distribution libraries and file system paths required to install zSecure. The storage requirements of zSecure 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 10. Storage Requirements for zSecure Target Libraries*

| Library DDNAME | Member Type | Target Volume | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|---|---|
| SCKRCARL | | ANY | U | PDS | FB | 80 | 286 | 58 |
| SCKRCLIB | EXEC | ANY | U | PDS | FB | 80 | 57 | 6 |
| SCKRLOAD | LMOD | ANY | U | PDSE | U | 0 | 867 | n/a |
| SCKRMLIB | MSG | ANY | U | PDS | FB | 80 | 12 | 7 |
| SCKRPAX | | ANY | U | PDS | FB | 80 | 236 | 2 |
| SCKRPLIB | PNL | ANY | U | PDSE | FB | 80 | 1614 | n/a |
| SCKRPROC | PROC | ANY | U | PDS | FB | 80 | 5 | 3 |
| SCKRSAMP | SAMP | ANY | U | PDS | FB | 80 | 29 | 9 |
| SCKRSLIB | SKEL | ANY | U | PDS | FB | 80 | 29 | 10 |
| SCKRTLIB | Table | ANY | U | PDS | FB | 80 | 45 | 2 |
| SCKRCJPN | EXEC | ANY | U | PDS | FB | 80 | 254 | 5 |
| SCKRMJPN | MSG | ANY | U | PDS | FB | 80 | 12 | 7 |

*Figure 11. Storage Requirements for zSecure Distribution Libraries*

| Library DDNAME | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|
| ACKRCARL | U | PDS | FB | 80 | 286 | 58 |
| ACKRCLIB | U | PDS | FB | 80 | 57 | 6 |
| ACKRLOAD | U | PDSE | U | 0 | 934 | n/a |
| ACKRMLIB | U | PDS | FB | 80 | 12 | 7 |
| ACKRPAX | U | PDS | FB | 80 | 236 | 2 |
| ACKRPLIB | U | PDSE | FB | 80 | 1614 | n/a |
| ACKRPROC | U | PDS | FB | 80 | 5 | 3 |
| ACKRSAMP | U | PDS | FB | 80 | 29 | 9 |
| ACKRSLIB | U | PDS | FB | 80 | 29 | 10 |
| ACKRTLIB | U | PDS | FB | 80 | 45 | 2 |
| ACKRCJPN | U | PDS | FB | 80 | 254 | 5 |
| ACKRMJPN | U | PDS | FB | 80 | 12 | 7 |
| AC4RLNK | S | PDSE | U | 0 | 12 | n/a |

The following figures list data sets that are not used by SMP/E, but are required for zSecure to run.

*Figure 12. Storage Requirements for zSecure Non-SMP/E Data Sets*

| Data Set Name | TYPE | ORG | RECFM | LRECL | No. of 3390 Trks | No. of DIR Blks |
|---|---|---|---|---|---|---|
| your.hlq.CKRJOBS | U | PDS | FB | 80 | 15 | 10 |
| your.hlq.CKRPARM | U | PDS | FB | 80 | 15 | 10 |
| your.hlq.CKRPROF | U | PDS | FB | 80 | 15 | 10 |
| your.hlq.CKACUST | U | PDS | FB | 80 | 30 | 20 |

## 5.3 FMIDs Deleted

Installing zSecure 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 zSecure 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

zSecure has no special considerations for the target system.

# 6.0 Installation Instructions

This chapter describes the installation method and the step-by-step procedures to install and to activate the functions of zSecure.

Please note the following points:

- If you want to install zSecure into its own SMP/E environment, consult the SMP/E manuals for instructions on creating and initializing the SMPCSI and the SMP/E control data sets. Additionally, to assist you in doing this, IBM has provided samples to help you create an SMP/E environment at the following url:
  http://www.ibm.com/support/docview.wss?uid=swg21066230

  Alternatively, you may want to use the Fast install process, as described in the Installation and Deployment Guide. Fast install will create its own SMP/E environment.
- Sample jobs have been provided to help perform some or all of the installation tasks. The SMP/E jobs assume that all DDDEF entries required for SMP/E execution have been defined in the appropriate zones.

  **Note:** If you want to install the Security zSecure Admin RACF-Offline function, you cannot use the "fast installation" process to install zSecure. The RACF-Offline function requires that the entire zSecure product is installed in the z/OS target and distribution zones. In that case you cannot install the products into their own global and target zones, but must use the same zones as used for the z/OS installation.
- The SMP/E dialogs may be used instead of the sample jobs to accomplish the SMP/E installation steps.

## 6.1 Installing zSecure

### 6.1.1 SMP/E Considerations for Installing zSecure

Use the SMP/E RECEIVE, APPLY, and ACCEPT commands to install this release of zSecure.

### 6.1.2 SMP/E Options Subentry Values

The recommended values for certain SMP/E CSI subentries are shown in Figure 13. 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 13. SMP/E Options Subentry Values*

| Subentry | Value | Comment |
|---|---|---|
| DSSPACE | (30,135,810) | Space Allocation for SMPTLIB data sets |
| PEMAX | SMP/E Default | IBM recommends using the SMP/E default for PEMAX. |

## 6.1.3 Sample Jobs

The following sample installation jobs are provided as part of the product to help you install zSecure:

*Figure 14. Sample Installation Jobs*

| Job Name | Job Type | Description | RELFILE |
|---|---|---|---|
| CKRZUPDZ | UPDATE | Sample job to update installation library | IBM.HCKR230.F1 |
| CKRZUPDI | - | Input data for job CKRZUPDZ. It is also used during post-install job CKRZPOST. | IBM.HCKR230.F1 |
| C2RIISPF | - | JCL-include for job CKRZUPDZ. It is also used during post-install job CKRZPOST, and as part of the installed product (the Change Tracking function) | IBM.HCKR230.F1 |
| CKRZSMPA | DEFINE | Sample job to create a Global CSI | IBM.HCKR230.F1 |
| CKRZSMPB | DEFINE | Sample job to create a Target/Dlib CSI | IBM.HCKR230.F1 |
| CKRZSMPC | DEFINE | Sample job to define an SMP/E OPTIONS entry | IBM.HCKR230.F1 |
| CKRZREC | RECEIVE | Sample RECEIVE job | IBM.HCKR230.F1 |
| CKRZALL | ALLOCATE | Sample job to allocate target and distribution libraries | IBM.HCKR230.F1 |
| CKRZDDD | DDDEF | Sample job to define SMP/E DDDEFs | IBM.HCKR230.F1 |
| CKRZAPP | APPLY | Sample APPLY job | IBM.HCKR230.F1 |
| CKRZACC | ACCEPT | Sample ACCEPT job | IBM.HCKR230.F1 |

You can access the sample installation jobs by performing an SMP/E RECEIVE (refer to 6.1.6, “Perform SMP/E RECEIVE” on page 19) then copy the jobs from the RELFILES to a work data set for editing and submission. See Figure 14 to find the appropriate relfile data set.

You can also copy the sample installation jobs from the directory where your Shopz order is stored by submitting the following job.

```
//STEP1 EXEC PGM=GIMUNZIP,REGION=0M,PARM='HASH=NO'
//SYSUT3 DD UNIT=SYSALLDA,SPACE=(CYL,(10,10))
//SYSUT4 DD UNIT=SYSALLDA,SPACE=(CYL,(15,5))
//SMPJHOME DD PATH='/usr/lpp/java/J5.0/'        <===NOTE 1
//SMPCPATH DD PATH='/usr/lpp/smp/classes/'      <===NOTE 1
//SMPOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SMPDIR DD PATHDISP=KEEP,
// PATH='/<ntsdir>/<orderid>/SMPRELF/'          <===NOTE 2
//SYSIN DD *
<GIMUNZIP>
<ARCHDEF
name="CBCACHE.IBM.HCKR230.F1.pax.Z"
volume="<volser>"                               <===NOTE 3
newname="<your-prefix>.CKRINST">                <===NOTE 4
</ARCHDEF>
</GIMUNZIP>
/*
```

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

Add a job card that is specific to your installation requirements.
Note 1: Change these directories to your installations java and smp classes directories.
Note 2: Change ntsdir to the directory that holds your Shopz orders. Change orderid to your order ID, for example 2008567304_000010_PROD.
Note 3: Change volser to a volser that you want the output dataset to reside on.
Note 4: Change your-prefix to the high-level qualifier(s) for the output dataset.

If you install from tape, refer to the documentation provided by CBPDO to see where IBM.HCKR230.F1 is on the tape. If you install through electronic shipment, refer to *CBPDO Internet Delivery User's Guide*.

## 6.1.4 Batch-mode Updating the jobs (optional)

In order to apply your naming convention, you can manually edit the install jobs. All zSecure-supplied jobs contain instructions on changing jobcards, data set names, high level qualifiers, etc.

A more convenient way to apply your naming convention is using update parameter member CKRZUPDI, JCL-include C2RIISPF, and global update job CKRZUPDZ. These are described in the Installation and Deployment Guide. In addition, job CKRZUPDZ uncomments the required FMIDs, according to the products you selected, in the RECEIVE, APPLY and ACCEPT jobs. Updating CKRZUPDI and C2RIISPF is optional for the Formal install process. However, we recommend that you do these updates, not only for convenience, but also because post-install job CKRZPOST makes use of these members. Member C2RIISPF, in its customized form, is also used as part of the installed product (the Change Tracking function).

## 6.1.5 Setup SMP/E CSI and Zones (optional)

For setting up the SMP/E environment, see the notes at the beginning of this chapter, or use the sample jobs mentioned above.

### 6.1.5.1 Allocate SMP/E GLOBAL CSI (Optional)

If you choose to install this product in its own SMP/E environment, edit and submit sample job CKRZSMPA to allocate a new SMP/E GLOBAL CSI.

**Expected Return Code and Messages:** This job should end with a return code 0.

### 6.1.5.2 Allocate SMP/E Target/DLIB CSI (Optional)

If you choose to install this product in its own SMP/E environment, edit and submit sample job CKRZSMPB to allocate a new SMP/E TARGET/DLIB CSI.

**Expected Return Code and Messages:** This job should end with a return code 0.

### 6.1.5.3 Define OPTIONS entry to SMP/E GLOBAL/Target/DLIB CSI (Optional)

If you choose to install this product in its own SMP/E environment, edit and submit sample job CKRZSMPC to create and specify an OPTIONS entry for use during installation of the product.

**Expected Return Code and Messages:** This job should end with a return code 0.

## 6.1.6 Perform SMP/E RECEIVE

Having obtained zSecure as part of a CBPDO, use the RCVPDO job found in the CBPDO RIMLIB data set to RECEIVE the zSecure FMIDs as well as any service, HOLDDATA, included on the CBPDO tape. For more information, refer to the documentation included with the CBPDO.

You can also choose to edit (if you did not use CKRZUPDZ) and submit sample job CKRZREC to perform the SMP/E RECEIVE for zSecure. Consult the instructions in the sample job for more information.

You should always RECEIVE FMIDs HCKR230 and HC4R230, and other FMIDs, according to table 1.2, “IBM Security zSecure Compliance and Auditing FMIDs” on page 2, or according to your choices in member CKRZUPDI. If you run job CKRZUPDZ, as described in section 6.1.4, “Batch-mode Updating the jobs (optional)” on page 18, the FMIDs that you need will already be uncommented. If you did not run CKRZUPDI, you need to uncomment the FMIDs yourself.

If you are installing multiple products of the zSecure suite from separate install media (as opposed to a single CBPDO tape or electronic download), you should at this point run job CKRZREC against all zSecure product tapes (or download files) before proceeding to the next job. If any messages "already received" arise, ignore them. Installing in this way gives you a single set of libraries with all the required capabilities. zSecure functions.

**Expected Return Codes and Messages:** This should issue a return code of zero and no error messages.

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

Edit (if you did not use CKRZUPDZ) and submit sample job CKRZALL to allocate the SMP/E target and distribution libraries for zSecure. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** This job will complete with a return code 4 if the AC4RLNK does not exist or return code 0 if it does. You must check allocation messages to verify the data sets are allocated and cataloged as expected.

### 6.1.8 Create DDDEF Entries

Edit (if you did not use CKRZUPDZ) and submit sample job CKRZDDD to create DDDEF entries for the SMP/E target and distribution libraries for zSecure. Consult the instructions in the sample job for more information.

**Expected Return Codes and Messages:** This should issue a return code of zero and no error messages.

### 6.1.9 Perform SMP/E APPLY

1. Ensure you have the latest Enhanced HOLDDATA, then edit (if you did not use CKRZUPDZ) and submit sample job CKRZAPP to perform an SMP/E APPLY CHECK for zSecure. Consult the instructions in the sample job for more information.

   The latest HOLDDATA is available through several different portals, including http://service.software.ibm.com/holdata/390holddata.html. 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 the 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.

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.

You should always APPLY FMIDs HCKR230 and HC4R230, and other FMIDs, according to table 1.2, “IBM Security zSecure Compliance and Auditing FMIDs” on page 2, or according to your choices in member CKRZUPDI. If you run job CKRZUPDZ, as described in section 6.1.4, “Batch-mode Updating the jobs (optional)” on page 18, the FMIDs that you need will already be uncommented. If you did not run CKRZUPDI, you need to uncomment the FMIDs yourself.

**Expected Return Codes and Messages from APPLY CHECK:** This should issue a return code of zero and no error messages.

**Expected Return Codes and Messages from APPLY:** This should issue a return code of zero and no error messages.

**Note!**

Using GROUPEXTEND in APPLY with maintenance with HOLDDATA may cause a return code other than 0.

After installing new functions, you should perform two operations:

1. Create a backup of the updated data sets, including any SMP/E data sets affected, in case something happens to the data sets during the next phase.
2. Do some testing before putting the new function into production.

After you are satisfied that an applied SYSMOD has performed reliably in your target system, you can install it in your distribution libraries using the ACCEPT process.

Another good practice is to accept most SYSMODs, particularly FMIDs, before performing another APPLY process. This provides you the ability to use the RESTORE process of SMP/E and to support the scenario where SMP/E needs to create a new load module from the distribution libraries during the APPLY process.

## 6.1.10 Perform SMP/E ACCEPT

Edit (if you did not use CKRZUPDZ) and submit sample job CKRZACC to perform an SMP/E ACCEPT CHECK for zSecure. Consult the instructions in the sample job for more information.

You should always ACCEPT FMIDs HCKR230 and HC4R230, and other FMIDs, according to table 1.2, “IBM Security zSecure Compliance and Auditing FMIDs” on page 2, or according to your choices in member CKRZUPDI. If you run job CKRZUPDZ, as described in section 6.1.4, “Batch-mode Updating the jobs (optional)” on page 18, the FMIDs that you need will already be uncommented. If you did not run CKRZUPDI, you need to uncomment the FMIDs yourself.

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 only *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:** This should issue a return code of zero and no error messages.

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:** This should issue a return code of zero and no error messages.

### 6.1.11 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 zSecure, 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 on REPORT CROSSZONE, see the SMP/E manuals.

## 6.2 Activating zSecure

### 6.2.1 Post install

The publication *IBM Security zSecure Suite: CARLa driven components,Installation and Deployment Guide Version 2.3.0, SC27-5638* contains the step-by-step procedures to fully activate the functions of zSecure. These steps include

- Copying to or connecting from your images
- Making the software APF authorized
- Check product enablement via IFAPRDxx in PARMLIB
- Making the software available to TSO/ISPF users
- Making the software available for batch processes
- Making configurations available

- Configuration
- Installation verification

# 7.0 Notices

References in this document to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

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 contact the IBM Customer Support Center or use S/390 SoftwareXcel to obtain the current "PSP Bucket".

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 online versions of this book, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

## 7.1 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" at www.ibm.com/legal/copytrade.shtml.

# Contacting IBM Software Support

For support for this or any IBM product, you can contact IBM Software Support as follows:

Submit a Service Request (SR, formerly called Problem Management Record or PMR) electronically from the support Web site at:

https://www.ibm.com/support/servicerequest/Home.action

You can also review the *IBM Software Support Handbook*, which is available on the Web site listed above. An *End of Support Matrix* is provided that tells you when products you are using are nearing the end of support date for a particular version or release.

When you contact IBM Software Support, be prepared to provide identification information for your company so that support personnel can readily assist you. Company identification information might also be needed to access various online services available on the Web site.

The support Web site offers extensive information, including a guide to support services (the *IBM Software Support Handbook*); frequently asked questions (FAQs); and documentation for all products, including Release Notes, Redbooks, and Whitepapers. The documentation for some product releases is available in both PDF and HTML formats. Translated documents are also available for some product releases.

Printed in USA

GI13-2294-06