

Security zSecure Manager for RACF z/VM  
Version 1.11.2

*Installation and Deployment Guide*





Security zSecure Manager for RACF z/VM  
Version 1.11.2

*Installation and Deployment Guide*



**Note**

Before using this information and the product it supports, read the information in Appendix C, "Notices," on page 37.

**Edition notice**

This edition applies to version 1, release 11, modification 2 of IBM Security zSecure Manager for RACF z/VM (product number 5655-T13) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 1989, 2015.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>About this publication</b> . . . . .	<b>v</b>
Access to publications and terminology . . . . .	v
Related documentation. . . . .	ix
Accessibility . . . . .	ix
Technical training . . . . .	ix
Support information. . . . .	x
Statement of Good Security Practices . . . . .	x
<b>Chapter 1. Installation roadmap</b> . . . . .	<b>1</b>
<b>Chapter 2. Installation overview</b> . . . . .	<b>3</b>
The default Start program: CKV . . . . .	3
The configuration file . . . . .	3
<b>Chapter 3. Preparing for installation</b> . . . . .	<b>5</b>
Verifying the release . . . . .	5
Evaluating space requirements . . . . .	5
Planning for a distribution-oriented installation. . . . .	5
<b>Chapter 4. Configuring zSecure Manager for RACF z/VM</b> . . . . .	<b>7</b>
Setting up the configuration file . . . . .	7
Selecting a configuration file . . . . .	7
Customizing installation option settings . . . . .	8
Building the CKRSITE load library . . . . .	9
Customizing options for user groups . . . . .	10
Customizing language settings and display text (SE.D.N) . . . . .	11
Customizing Menu items. . . . .	13
Customizing action line commands . . . . .	15
Adding and selecting CARLa command libraries (SE.D.8). . . . .	19
Setting up rule-based compliance evaluations (option AU.R) . . . . .	20
<b>Chapter 5. Making the software available in CMS</b> . . . . .	<b>21</b>
Upgrading the product for CMS users . . . . .	21
Establishing the start method for CMS users . . . . .	22
<b>Chapter 6. Setting up for production</b> . . . . .	<b>23</b>
Capacity planning . . . . .	23
DASD storage . . . . .	23
Virtual storage . . . . .	24
CPU time . . . . .	24
Network load. . . . .	25
Specifying the default input set. . . . .	25
Setting up the daily collection process . . . . .	25
Data collection parameters . . . . .	25
Refreshing the CKFREEZE file . . . . .	27
<b>Chapter 7. Verifying the installation</b> . . . . .	<b>29</b>
<b>Appendix A. Configuration parameters</b> . . . . .	<b>31</b>
<b>Appendix B. Setting up and starting a CMSBATCH server</b> . . . . .	<b>35</b>
<b>Appendix C. Notices</b> . . . . .	<b>37</b>
Trademarks . . . . .	39
<b>Index</b> . . . . .	<b>41</b>



---

## About this publication

This manual describes the installation and configuration processes for Version 1.11.2 of the IBM Security zSecure Manager for RACF z/VM product.

The manual provides instructions for installing, configuring, and deploying the software. It describes the REXX program for starting the product and the configuration files for customizing installation options and other settings.

This publication is intended for people who install, configure, deploy, and maintain IBM Security zSecure Manager for RACF z/VM.

Readers must be familiar with the operating system where the product is being installed.

---

## Access to publications and terminology

This section provides:

- A list of publications in the “IBM Security zSecure Manager for RACF z/VM library” and the “IBM Security zSecure library” on page vi.
- Links to “Online publications” on page viii.
- A link to the “IBM Terminology website” on page ix.

### IBM Security zSecure Manager for RACF z/VM library

The following documents are available in the IBM Security zSecure Manager for RACF z/VM library:

- *IBM Security zSecure Manager for RACF z/VM Release Information*  
For each product release, the Release Information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information. You can obtain the most current version of the Release Information at [http://www.ibm.com/support/knowledgecenter/SSQQGJ\\_1.11.2/com.ibm.zsecurevm.doc\\_1.11.2/welcome.html](http://www.ibm.com/support/knowledgecenter/SSQQGJ_1.11.2/com.ibm.zsecurevm.doc_1.11.2/welcome.html).
- *IBM Security zSecure Manager for RACF z/VM: Installation and Deployment Guide, SC27-4363*  
Provides information about installing, configuring, and deploying the product.
- *IBM Security zSecure Manager for RACF z/VM User Reference Manual, LC27-4364*  
Describes how to use the product interface and the RACF<sup>®</sup> administration and audit functions. The manual provides reference information for the CARLa command language and the SELECT/LIST fields. It also provides troubleshooting resources and instructions for using the zSecure Collect component. This publication is available only to licensed users.
- *IBM Security zSecure CARLa Command Reference, LC27-6548*  
Provides both general and advanced user reference information about the CARLa Auditing and Reporting Language (CARLa). CARLa is a programming language that is used to create security administrative and audit reports with zSecure<sup>™</sup>. The *CARLa Command Reference* also provides detailed information about the NEWLIST fields for selecting data and creating zSecure reports. This publication is available only to licensed users.
- *IBM Security zSecure Messages Guide, SC27-6549*

Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.

- *IBM Security zSecure Manager for RACF z/VM Documentation CD, LCD8-2726*  
Supplies the IBM Security zSecure documentation, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is available only to licensed users.
- *Program Directory for IBM Security zSecure Manager for RACF z/VM, GI11-7865*  
The *Program Directory for IBM Security zSecure Manager for RACF z/VM* is intended for the systems programmer responsible for installing, configuring, and deploying the product. It contains information about the materials and procedures associated with installing the software. The Program Directory is provided with the product tape. You can also download the latest copy from the IBM Knowledge Center available at [http://www.ibm.com/support/knowledgecenter/SSQQGJ\\_1.11.2/com.ibm.zsecurevm.doc\\_1.11.2/welcome.html](http://www.ibm.com/support/knowledgecenter/SSQQGJ_1.11.2/com.ibm.zsecurevm.doc_1.11.2/welcome.html).

## IBM Security zSecure library

The following documents are available online in the IBM Security zSecure library:

- *IBM Security zSecure Release information*  
For each product release, the release information topics provide information about new features and enhancements, incompatibility warnings, and documentation update information for the IBM Security zSecure products. You can obtain the most current version of the release information at [http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html).
- *IBM Security zSecure CARLa-Driven Components Installation and Deployment Guide, SC27-5638*  
Provides information about installing and configuring the following IBM Security zSecure components:
  - IBM Security zSecure Admin
  - IBM Security zSecure Audit for RACF, CA-ACF2, and CA-Top Secret
  - IBM Security zSecure Alert for RACF and ACF2
  - IBM Security zSecure Visual for RACF
  - IBM® Security zSecure Adapters for QRadar SIEM for RACF, CA-ACF2, and CA-Top Secret
- *IBM Security zSecure Admin and Audit for RACF Getting Started, GI13-2324*  
Provides a hands-on guide introducing IBM Security zSecure Admin and IBM Security zSecure Audit product features and user instructions for performing standard tasks and procedures. This manual is intended to help new users develop both a working knowledge of the basic IBM Security zSecure Admin and Audit for RACF system functionality and the ability to explore the other product features that are available.
- *IBM Security zSecure Admin and Audit for RACF User Reference Manual, LC27-5639*  
Describes the product features for IBM Security zSecure Admin and IBM Security zSecure Audit. Includes user instructions to run the features from ISPF panels, RACF administration and audit user documentation with both general and advanced user reference material for the CARLa command language and the SELECT/LIST fields. This manual also provides troubleshooting resources



and instructions for installing the zSecure Collect for z/OS component. This publication is only available to licensed users.

- *IBM Security zSecure Audit for ACF2 Getting Started*, GI13-2325  
Describes the IBM Security zSecure Audit for ACF2 product features and provides user instructions for performing standard tasks and procedures such as analyzing Logon IDs, Rules, and Global System Options, and running reports. The manual also includes a list of common terms for those not familiar with ACF2 terminology.
- *IBM Security zSecure Audit for ACF2 User Reference Manual*, LC27-5640  
Explains how to use IBM Security zSecure Audit for ACF2 for mainframe security and monitoring. For new users, the guide provides an overview and conceptual information about using ACF2 and accessing functionality from the ISPF panels. For advanced users, the manual provides detailed reference information including message and return code lists, troubleshooting tips, information about using zSecure Collect for z/OS, and details about user interface setup. This publication is only available to licensed users.
- *IBM Security zSecure Audit for Top Secret User Reference Manual*, LC27-5641  
Describes the IBM Security zSecure Audit for Top Secret product features and provides user instructions for performing standard tasks and procedures.
- *IBM Security zSecure CARLa Command Reference*, LC27-6533  
Provides both general and advanced user reference information about the CARLa Auditing and Reporting Language (CARLa). CARLa is a programming language that is used to create security administrative and audit reports with zSecure. The *CARLa Command Reference* also provides detailed information about the NEWLIST fields for selecting data and creating zSecure reports. This publication is available only to licensed users.
- *IBM Security zSecure Alert User Reference Manual*, SC27-5642  
Explains how to configure, use, and troubleshoot IBM Security zSecure Alert, a real-time monitor for z/OS® systems protected with the Security Server (RACF) or CA-ACF2.
- *IBM Security zSecure Command Verifier User Guide*, SC27-5648  
Explains how to install and use IBM Security zSecure Command Verifier to protect RACF mainframe security by enforcing RACF policies as RACF commands are entered.
- *IBM Security zSecure CICS Toolkit User Guide*, SC27-5649  
Explains how to install and use IBM Security zSecure CICS Toolkit to provide RACF administration capabilities from the CICS® environment.
- *IBM Security zSecure Messages Guide*, SC27-5643  
Provides a message reference for all IBM Security zSecure components. This guide describes the message types associated with each product or feature, and lists all IBM Security zSecure product messages and errors along with their severity levels sorted by message type. This guide also provides an explanation and any additional support information for each message.
- *IBM Security zSecure Quick Reference*, SC27-5646  
This booklet summarizes the commands and parameters for the following IBM Security zSecure Suite components: Admin, Audit, Alert, Collect, and Command Verifier. Obsolete commands are omitted.
- *IBM Security zSecure Visual Client Manual*, SC27-5647  
Explains how to set up and use the IBM Security zSecure Visual Client to perform RACF administrative tasks from the Windows-based GUI.
- *IBM Security zSecure Documentation CD*, LCD8-2726

Supplies the IBM Security zSecure documentation, which contains the licensed and unlicensed product documentation. The *IBM Security zSecure: Documentation CD* is available only to licensed users.

- *Program Directory for IBM Security zSecure Suite: CARLa-driven components*, GI13-2277

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CARLa-Driven Components: Admin, Audit, Visual, Alert, and the IBM Security zSecure Adapters for QRadar SIEM. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at [http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html).

- *Program Directory for IBM Security zSecure CICS Toolkit*, GI13-2282

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure CICS Toolkit. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at [http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html).

- *Program Directory for IBM Security zSecure Command Verifier*, GI13-2284

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of IBM Security zSecure Command Verifier. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at [http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html).

- *Program Directory for IBM Security zSecure Admin RACF-Offline*, GI13-2278

This program directory is intended for the system programmer responsible for program installation and maintenance. It contains information concerning the material and procedures associated with the installation of the IBM Security zSecure Admin RACF-Offline component of IBM Security zSecure Admin. Program directories are provided with the product tapes. You can also download the latest copy from the IBM Security zSecure documentation website at [http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html).

## Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

### **IBM Security zSecure Manager for RACF z/VM library**

The product documentation site ([http://www.ibm.com/support/knowledgecenter/SSQQGJ\\_1.11.2/com.ibm.zsecurevm.doc\\_1.11.2/welcome.html](http://www.ibm.com/support/knowledgecenter/SSQQGJ_1.11.2/com.ibm.zsecurevm.doc_1.11.2/welcome.html)) displays the welcome page and navigation for the library.

### **IBM Security zSecure library**

The product documentation site ([http://www.ibm.com/support/knowledgecenter/SS2RWS\\_2.1.1/com.ibm.zsecure.doc\\_2.1.1/welcome.html](http://www.ibm.com/support/knowledgecenter/SS2RWS_2.1.1/com.ibm.zsecure.doc_2.1.1/welcome.html)) displays the welcome page and navigation for the library.

### IBM Security Systems Documentation Central

IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

### IBM Publications Center

The IBM Publications Center site (<http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss>) offers customized search functions to help you find all the IBM publications you need.

### IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

---

## Related documentation

If you are using IBM Security zSecure products in a RACF environment, you can find RACF user and reference information in several IBM manuals. For information about the RACF commands, and the implications of the various keywords, see the *RACF Command Language Reference* and the *RACF Security Administrator's Guide*. For information about writing other RACF exits, see the *RACF System Programmer's Guide*. You can find information about auditing RACF in the *RACF Auditor's Guide*. You can access this documentation in the IBM Knowledge Center at <http://www.ibm.com/support/knowledgecenter/SSB27U/welcome>. Also see <http://www.vm.ibm.com/library> for more information about z/VM.

*Table 1. Further information about RACF administration, auditing, programming, and commands*

Manual	Order Number
<i>z/VM RACF Security Server Command Language Reference</i>	SC24-6213
<i>z/VM RACF Security Server Security Administrator's Guide</i>	SC24-6218
<i>z/VM RACF Security Server Auditor's Guide</i>	SC24-6212
<i>z/VM RACF Security Server System Programmer's Guide</i>	SC24-6219
<i>ISPF Quick Start Guide for VM V2R3</i>	GI13-3554

---

## Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

---

## Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

---

## Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

---

## Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

---

# Chapter 1. Installation roadmap

## About this task

Table 2 provides an overview of the steps to install, configure, and deploy a new installation of IBM Security zSecure Manager for RACF z/VM.

Table 2. Installation roadmap

Task description	See...
Learn about key concepts and resources related to installing, configuring, and deploying the product. <ol style="list-style-type: none"><li>1. Review the concepts of single installation and distribution-oriented installation.</li><li>2. Learn about CKV, the default REXX program (CKV SAMPLE) that starts the product and the default configuration file (C2R\$PARV SAMPLE) that specifies initial configuration settings.</li></ol>	Chapter 2, "Installation overview," on page 3
Prepare for installation: <ol style="list-style-type: none"><li>1. Verify the release.</li><li>2. Evaluate space requirements.</li><li>3. Plan for distribution-oriented installation.</li></ol>	Chapter 3, "Preparing for installation," on page 5
Install the software using the <i>Program Directory for IBM Security zSecure Manager for RACF z/VM</i> .	Information center for IBM Security zSecure Manager for RACF z/VM
Configure the product: <ol style="list-style-type: none"><li>1. Set up the configuration file.</li><li>2. Update the Start program with the software location and configuration file name.</li><li>3. Optional. Customize installation-defined settings.</li><li>4. Optional. Use the Setup Default option from the product menu to customize language settings, display text, menu options, and line commands for user groups.</li></ol> <p><b>Note:</b> Depending on the installation, you might need multiple copies of the configuration file and the Start program.</p>	Chapter 4, "Configuring zSecure Manager for RACF z/VM," on page 7
Make the software available in CMS: <ol style="list-style-type: none"><li>1. Make sure that the REXX program that starts the product is available in a location that CMS users can access.</li><li>2. Establish a start procedure for CMS users.</li></ol>	Chapter 5, "Making the software available in CMS," on page 21
Set up for production: <ol style="list-style-type: none"><li>1. Review the capacity planning information to help you determine the system resources required.</li><li>2. Specify the default input set.</li><li>3. Set up the daily collection job.</li><li>4. Refresh the CKFREEZE file.</li></ol>	Chapter 6, "Setting up for production," on page 23
Verify the installation: <ol style="list-style-type: none"><li>1. Check the base UI functions.</li><li>2. Check the zSecure Collect function.</li><li>3. Check installation-defined option settings.</li></ol>	Chapter 7, "Verifying the installation," on page 29



---

## Chapter 2. Installation overview

The installation, configuration, and deployment process supports both single and distribution-oriented installation.

- In a single installation, you install zSecure Manager for RACF z/VM separately on each z/VM<sup>®</sup> image.
- In a distribution-oriented installation, you install the product on one z/VM image, and then run it on multiple images using different configuration files. You can also run multiple configurations in a single z/VM image. For example, you can provide central administrators with access to a full-function configuration. You can provide site administrators with access to a streamlined configuration that includes only the Quick Administration Menu (option **RA.Q**).

**Note:** If you need to perform RACF administration and auditing tasks on both z/VM and z/OS systems, you must install zSecure separately for each operating system. For information about installing the z/OS version of the product, see *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

Two key components of the software configure and deploy the product in your environment: the default Start program and one or more configuration files.

---

### The default Start program: CKV

IBM Security zSecure Manager for RACF z/VM provides the CKV REXX program to start the product on a z/VM system. This file is shipped as CKV SAMPLE as a sample file on the production build disk, which might be called 5655T13D 200 disk.

This program links and accesses the minidisk where the software is installed. It also provides a pointer to the default configuration file for running the product. The program is provided on the production build disk. This file includes the following code.

```
configurationFile      = 'C2R$PARV CKVPARAM *'  
codeMiniDisk          = '5655T13D 200'
```

You can set up multiple Start programs for different systems and User groups.

---

### The configuration file

A configuration file specifies the configuration options for a specific instance of the software. Depending on installation requirements, you can create multiple versions of the configuration file for different systems and User groups. You can select the configuration file that establishes the initial product settings in the Start program, or as a passed parameter on the program start command.

Store the configuration files separately from the installed software so that the modifications are not overwritten during product upgrades.

C2R\$PARV SAMPLE is a sample configuration file on the production build disk, which might be called 5655T13D 200 disk. This file includes the following code:

```

workFileMode      ='A'           /* Mode for new (scratch) files */
customizationFileMode ='B'       /* Filemode with C2RPROF files */
description        ='Default files' /* Description for input set */
unload            =' '          /* Unloaded RACF database */
ckfreeze          =' '          /* fn ft fm of CKFREEZE */
smf               =' '          /* fn ft fm of SMF */
init              ='NO'         /* initialize every time */
userLibFileMode   =' '          /* file mode user ISPF libraries */
earlyWrn          =' '          /* ids to receive conf.error msgs */
ISPFMiniDisk      ='ISPM 192'    /* Minidisk with ISPF code */
CKACUSTMiniDisk   =' '          /* User/Minidisk with site CKACUST*/
racfDBCMS         ='DBCOPY RACF A' /* RACF db in CMS minidisk format */
racfDbDataset     ='RACF.DATASET' /* OS dsname of RACF database */
racfMiniDisk      ='RACFVM 200'   /* Minidisk with RACF database */
racfVirtualAddress =freeaddr     /* Virt addr to access RACF db */
racfFileMode      =freemode      /* Mode to access RACF db */
mode              = 'ISPF'       /* Mode to start zSecure in */

```

The examples in this publication use the convention that the C2R\$PARV SAMPLE file was copied to another location and renamed to C2R\$PARV CKVPARM.

Typically, configuration files are available on minidisks that are separate from the software. zSecure Manager for RACF z/VM never updates the files containing the actual software. Consequently, the minidisks with software are linked in read-only mode.



---

## Chapter 3. Preparing for installation

Before you install the product, see the following sections:

- Verify the release
- Evaluate space requirements
- Plan for a distribution-oriented installation

---

### Verifying the release

Verify that the product and release you are about to install is the current and supported release. Confirm that it is supported on the platform where you intend to use it. For information about the IBM Software Support Lifecycle, see [http://www.ibm.com/software/support/lifecycle/index\\_a\\_z.html](http://www.ibm.com/software/support/lifecycle/index_a_z.html).

---

### Evaluating space requirements

For programming and space requirements, see the *Program Directory for IBM Security zSecure Manager for RACF z/VM*. This document is available with the product, and online at [http://www.ibm.com/support/knowledgecenter/SSQQJ\\_1.11.2/com.ibm.zsecurevm.doc\\_1.11.2/welcome.html](http://www.ibm.com/support/knowledgecenter/SSQQJ_1.11.2/com.ibm.zsecurevm.doc_1.11.2/welcome.html).

---

### Planning for a distribution-oriented installation

If you are performing a distribution-oriented installation, review the following considerations:

- Consider the number of separate configurations you want to set up for users. For example, do you want to provide one configuration for Administrators and another for Operators?  
Each configuration requires a separate configuration file that specifies the required settings. These configuration files must be accessible to the program that starts the product.
- For each z/VM image to which you want to deploy the software, make sure that you have the information required to link and access the minidisk.  
Each z/VM image targeted for deployment must have a separate start program that points to the correct minidisk location and configuration file. You can override the configuration file specified in the start program by passing the configuration file name as a parameter on the start program.
- Decide where to store the customized start program and configuration files for each instance.

For information about customizing the configuration files and the REXX program that starts the product, see *Configure the product*.



---

## Chapter 4. Configuring zSecure Manager for RACF z/VM

The following topics describe how to set up, configure, and customize the product.

- Set up the configuration files
- “Selecting a configuration file”
- Customize installation options
- Customize options for user groups

---

### Setting up the configuration file

After installing the software, the default configuration file sample (C2R\$PARV SAMPLE) is available on the production build disk. You must copy this file to another location and use it to create the configuration files required in your environment.

To set up the configuration file, do the following steps:

1. Copy C2R\$PARV SAMPLE as C2R\$PARV CKVPARM to the local tools minidisk or another location that is accessed by the users.
2. Rename the file to C2R\$PARV CKVPARM or another name that you prefer.  
To use this default configuration file, skip to “Selecting a configuration file.”
3. To customize the configuration, edit the C2R\$PARV CKVPARM file to modify the parameters.
4. Save the modified file with a different name on a minidisk that is accessed and linked before starting the product.
5. Repeat these steps for each required configuration file.

Use the configuration files you created to establish the initial settings when the product starts. For more information, see the following topics:

- Appendix A, “Configuration parameters,” on page 31
- “Selecting a configuration file”

---

### Selecting a configuration file

You can select the configuration file for the product using the start program. You can also select the file at run time by specifying the file name in the CONFIG parameter on the product start command.

**Note:** These examples use CKV, the default REXX program that starts the product. This file is shipped as CKV SAMPLE as a sample file on the production build disk, which might be called 5655T13D 200 disk. Because the software supports multiple configurations, each installation can have a unique start program name. For example, you might have one start program for administrators called CKVADM and another for help desk personnel called CKVHLP. The start command name matches the program name. Copy CKV SAMPLE as CKV EXEC (or as any other command name) to the local tools minidisk or another location that is accessed by the users.

#### Specifying the configuration file name in the start command

Run the following command.

```
CKV (CONFIG = configfilename configfiletype configfilemode)
```

where

*configfilename* is the file name, *configfiletype* is the file type, and *configfilemode* is the file mode. Use an asterisk (\*) for the *filemode* value to specify a flexible location for the minidisk.

### Using the default configuration file specified in the start program

Run the following command.

```
CKV
```

If you run the start command without any parameters, the product starts using the configuration file specified in the `configurationFile` parameter in the CKV start program. For information about customizing this value, see [Make the software available to CMS users](#).

For more information, see the following topics:

[Set up the configuration files](#)

[Make the software available to CMS users](#)

---

## Customizing installation option settings

Table 3 describes the default product installation options specified by the CKRSITE parameters in the CKRCARLA load library. You can customize the default values for these options by building a separate CKRSITE load library and changing the values. Customizing these parameters is optional. The product is fully operational without changing these settings. For information, see [Build the CKRSITE Load Library](#).

*Table 3. Site module options*

Parameter	Valid values	Description	Default
AUTH	SINGLE DOUBLE TRIPLE	This parameter is not supported by zSecure Manager for RACF z/VM.	SINGLE
CUSTSPEC	Up to 100 characters of text	Site or customer-specific identifier. This parameter is included in the SYSPRINT output for zSecure Manager for RACF z/VM.	
CLASS	SAF class name	Resource class for the zSecure security checks. Under VM/CMS, the only resource checked is CKR.READALL.	XFACILIT
KEEPCOMMAND	Numeric	This parameter is not supported by zSecure Manager for RACF z/VM.	7
KEEPAUDIT	Numeric	This parameter is not supported by zSecure Manager for RACF z/VM.	30
RESTRICT	Y N	Restricted mode. Alternatively, use the general resource CKR.READALL provided by the CLASS parameter instead of this setting.	N

**Restricted mode** You can use zSecure Manager for RACF z/VM in two distinct modes: *unrestricted* and *restricted*.

- In *unrestricted* mode, all data in the RACF security database is included in reports that can be viewed from the ISPF panel or from printed reports.
- In *restricted* mode, only the data within the scope of the user ID is available. For example, in *restricted* mode a Help Desk operator cannot create the same reports or view the same data that a Central Administrator can.

Under VM/CMS, *restricted* mode does not provide full protection of information based on user scope. If a user has READ access to the disk where the RACF

database is stored, the user can read the database with zSecure or any other program. In these other programs, information might not be restricted.

Full restricted mode is supported under z/OS using the Program Access to Data Sets (PADS) feature. If your RACF database is shared between z/VM and z/OS, you can use full-restricted mode by accessing the RACF database only from the z/OS side and only in PADS mode. To do so, create the CKFREEZE files on the z/VM system. Then, transfer these files to the z/OS system and use them as the data source for RACF administration and auditing.

**Conditions for restricted mode** Restricted mode operation is determined by the access that the live system grants the user for the CKR.READALL resource in the XFACILIT class.

- NO access enforces restricted mode.
- READ access grants unrestricted mode

**Note:** The XFACILIT class is the default class specified for zSecure. (If you customized the CKRSITE module, the CLASS might be different.) However, the XFACILIT class is not enabled by default on z/VM systems. If the XFACILIT class is not yet enabled, use the following command to enable it:

```
RAC SETROPTS CLASSACT(XFACILIT) GENERIC(XFACILIT)
```

If zSecure cannot determine the access level for the CKR.READALL class because the resource is not covered by a profile, zSecure determines the restricted mode setting by the following process:

- If the installation options use the default setting CLASS=XFACILIT, restricted mode is in effect.
- Evaluate the return code (RC) for the CLASS setting in the RACF Class Descriptor Table (CDT). The mode is determined based on the following RC values:
  - RC=0: no restrictions
  - RC=4: RACF does not know. Check the RESTRICTED installation option in the CKRSITE module.
  - RC=8: restricted access
- If the CKRSITE module specifies RESTRICTED=YES, restricted mode is in effect.

For more information about restricted mode, see the *IBM Security zSecure CARLa-Driven Components: Installation and Deployment Guide*.

## Building the CKRSITE load library

### About this task

This optional procedure describes the steps to build a CKRSITE load library and change the default installation options. Perform this procedure if you want to change these options. Because this process uses assembler source code in the product, you need some knowledge of assembly language.

**Note:**

1. Using the CKRSITE module is optional. The product is fully operational without it.
2. If you use the CKRSITE module and customize it, you must rebuild it if you apply any service to the CKRSITE ASSEMBLE or the associated CKRSITED macro.

To build the CKRSITE load library, do the following steps:

## Procedure

1. Review Table 3 on page 8 to note which CKRSITE parameters require custom values.
2. Run the following commands to copy the supplied assembler source part from the production build disk where the product is installed.

```
LINK 5655T13D 200 ACF RR
ACCESS ACF E
COPYFILE CKRSITE ASSEMBLE E CKRSITE ASSEMBLE A
```

The preceding example copies the code from the default minidisk specified in the Program Directory, 5655T13D 200. You can also copy the code from the minidisk specified in the CodeMiniDisk parameter in the REXX program that starts the product (CKV).

3. In the CKRSITE ASSEMBLE file on the A disk, change the CKRSITE parameter values as noted in Step 1.
4. Run the REXX program CKVESITE to assemble, link edit, and build the CKRSITE load library on the A disk.
5. If any assembler errors occur, correct them and rerun the CKVESITE program as many times as necessary to resolve the errors.
6. Make sure that the CKRSITE load library is available when the product is started.
  - If the customizationFileMode parameter in the product configuration file specifies the value for a specific minidisk, copy the CKRSITE load library to the same disk.
  - If this variable is not defined, copy the CKRSITE load library to a minidisk available to all users of this product.
7. Check the CKRSITE load library during the installation verification process.

## Results

For additional information, see the following topics:

Appendix A, "Configuration parameters," on page 31

Check installation-defined option settings for CKGRACF operations

---

## Customizing options for user groups

Use the Setup Default (**SE.D**) option to customize program operation for different systems and different user groups.

Any changes you specify during the Setup process apply to the configuration files on the minidisk indicated in the customizationFileMode parameter in the configuration file. If you use a single customizationFileMode minidisk, the Setup Default option establishes system-wide option settings. If you do not change any of the default options, zSecure uses the default settings for the product.

You can configure the product so that the updated settings apply to all users or apply only when a new user logs in.

To minimize service availability issues during the customization process, do the following steps:

1. Specify the Setup Default options for a new minidisk.
2. Test the settings.

3. After confirming that the options are correct, swap the minidisks or copy the configuration file to the production system.

For more information, see the following topics:

- Change the default installation options
- Customize language settings and display text
- Customize Menu items
- Customize action line commands
- Add and select CARLa command libraries

## Changing the default installation options (SE.D)

### About this task

To change the default installation options, do the following steps:

### Procedure

1. Start ISPF with the selected customizationFileMode minidisk: Run the product start command with a configuration file that specifies customizationFileMode = 'x', or override the configuration when you start CKV. For more information, see "Selecting a configuration file" on page 7.
2. From the Main menu, type SE.D on the command line.
3. From the Setup panel, use the available options to change the Setup options. See Customize language settings and display text for information, or press F1 for help.
4. Press F3 to exit the SETUP panel.
5. At the prompt, type one of the following options to process the changes:
  - N applies the updated settings only to new users.
  - Y applies the updated settings to all users when they log in.
  - D discards all changes made. Changes to input file options, National Language settings, and input file selections cannot be discarded.

**Note:** To apply the default settings each time a user logs on, specify INIT=YES in the configuration file.

## Customizing language settings and display text (SE.D.N)

Use the Setup Default - NLS option (SE.D.N) to set language options for the product. You can also customize the display text and other settings for menu items and line commands.

Figure 1 on page 12 shows the Setup - NLS panel for customizing the options.

```

zSecure - Setup - NLS (- System defaults)
Command ==>
Change language to          Action on language items
1 1. English                1 1. No action (use specified language)
  2. Dutch                  2. Reset all items to company default
  3. French                 3. Reset all items to Security zSecure default
  4. German                 4. Customize Menu items
  5. Italian                5. Customize action line commands
  6. Portuguese
  7. Spanish
  8. Other
  0. Security zSecure

Language used: Default English

```

Figure 1. Setup - NLS panel

From the Setup - NLS panel, you can perform the following tasks:

- Select the language for the product interface.
- Reset the language and menu configuration to installation-defined options, or to the Security zSecure product defaults.
- Customize display text, descriptions, and processing behavior for menu items and line commands.

**Note:** When working with IBM Software Support, set the language to the default setting, Security zSecure. You can switch the language back to the one specified for your installation after resolving the support issue.

The following list describes the fields available on the Setup - NLS panel:

**Change language to** Specifies the language used for the product Menu panels and Action commands in the product interface. (When you are working with IBM Software Support, set the language to the default setting, Security zSecure.)

**Action on language items** specifies the operation to perform when you press Enter. Table 4 describes the available actions.

Table 4. Actions available for selecting and customizing language and display options

Action	Description
<b>1. No action (use specified language)</b>	Sets the language to the specified value and exits the Setup - NLS panel.
<b>2. Reset all items to company defaults</b>	Resets the settings to the system default values specified for your installation. If you have not specified any site-specific settings, the zSecure default configuration is used.
<b>2. Reset all items to zSecure defaults</b>	Resets all language and display options to the zSecure default values and exits the Setup - NLS panel.
<b>3. Customize Menu items</b>	Opens a panel for customizing the display text and processing behavior for menu items. For more information, see Customize Menu items.
<b>4. Customize action line commands</b>	Opens a panel for customizing display text and processing behavior for line commands. For more information, Customize action line commands.



## Customizing Menu items

You can customize Menu items in the following ways:

- Change the option characters for selecting an item.
- Change the short or long description.
- Add or delete an item.
- Advanced users can customize the command to run or the panel to open when a Menu item is selected.

Perform the following steps to customize a Menu item.

1. From the Setup menu, type **SE.D** to display the Setup Defaults panel.
2. Type **N** to display the Setup - NLS panel.
3. In the **Action on language items** field, type **4 (Customize Menu items option)**.
4. Press Enter to display the Menu item list panel shown in Figure 2.

```

zSecure - Setup - NLS (- SYSTEM DEFAULT ROW 1 OF 246
Command ==>                               Scroll ==> CSR
Specify action for menu item(s): Edit, Insert, Copy, Delete
Standard options  Option and text as shown on panel
- SE              SE Setup          Options and input data sets
- SE 0            0 Run              Specify run options
- SE 1            1 Input files     Select and maintain sets of input data set
- SE 2            2 New files       Allocate new data sets for UNLOAD and CKFR
- SE 3            3 Preamble        CARLa Commands run before every query
- SE 4            4 Confirm         Specify command generation options
- SE 5            5 View            Specify view options
- SE 7            7 Output          Specify output options
- SE 8            8 Command files   Select and maintain command library
- SE E            E E-mail          Configure e-mail address lists
- SE U            U User defined    User defined input sources
- SE C D          D Data sets       Maintain lists of sensitive data sets
- SE C M          M Site msgs       Site defined message table
- SE C C          C zSecure msgs    zSecure defined message table
- SE N            N NLS             National language support
- SE T            T Trace           Set trace flags and CARLa listing for diag
- SE V            VM VM Files       Copy RACF/VM database (VM only)

```

Figure 2. Customizing selection options from the Setup - NLS panel

5. To work with a Menu item, type one of the following commands in the Menu item selection field:
  - **E** to edit the settings for an existing item.
  - **I** to add a Menu item.
  - **C** to copy a Menu item entry as a template for creating an item.
  - **D** to delete a Menu item.
6. Press Enter.
7. On the Menu item specification panel, specify the Menu item settings. For more information, see “Menu Item specification panel” on page 14.
8. Press Enter to save the changes and return to the Menu item list panel.
9. Repeat steps 5 - 8 for each Menu item that you want to customize.
10. Press F3 to exit.
11. At the prompt, type one of the following options to process the changes:
  - N** applies the updated settings only to new users.
  - Y** applies the updated settings to all users when they log in.

## Menu Item specification panel

Figure 3 shows the panel for customizing Menu item settings. This panel is displayed when you edit, copy, insert, or delete a Menu item on the Setup - NLS Line command list panel shown in Figure 2 on page 13.

```

zSecure - Setup - NLS (- SYSTEM DEFAULTS)
Command ==>
Official option . . SE 0          (also used for profile checking)

Specify action for Menu item
1 1. Use as specified below      2. Delete Menu item
3. Reset to system defaults     4. Reset to zSecure defaults

Menu option . . . . 0          (as displayed on user menu)
Short description . . Run
Long description . . Specify run options
Command (or MENU) . CMD(%C2REDFLL NO &C2RNSE0)
Panel for "MENU" . . _____ New menu . . N (Y/N)

Press ENTER to continue.

```

Figure 3. Setup NLS options - Menu item specification panel

Use the following option and field descriptions to customize the Menu item and process the changes.

### Official option

Provides the link to the System Authorization Facility (SAF) resource, which is checked for this Menu item. The specification also determines the order of the Menu items on the Menu panels. You can specify a three-level deep value. For example, specifying RA 4 2, places the option on the **RA.4** menu.

You can change the Official option value only when you initially define a Menu item. To change the value for an existing Menu item, use the Copy and Insert line commands to create an entry that you can modify.

The product provides a set of default Menu items. If you add a new Menu item, include at least one of the following characters: @, #, or \$ in the **Official option** value. These characters identify installation-defined items. If the value does not contain one of these characters, the Menu item is deleted when an NLS upgrade is applied.

### Specify action for menu item

Specifies how to process the Menu item when you press Enter. Table 5 explains the available options.

Table 5. Actions available for selecting and customizing language and display options for Menu items

Action	Description
<b>1. Use as specified below</b>	Applies the menu items settings and exits the panel.
<b>2. Delete menu item</b>	Deletes the selected Menu item and exits the panel.
<b>3. Reset all items to system defaults</b>	Resets the Menu item to the system default descriptions and behavior and exits the panel. If no defaults have been specified, the product runs with the zSecure default configuration.
<b>4. Reset to zSecure defaults</b>	Resets the Menu item to the original product settings for the language specified.

### Menu option

Specifies the Menu option value to show on the Menu panel. You can specify multiple Menu items that have the same option value with different configurations. Use this configuration to provide the same option value for different profiles. For example, one group of users sees the first menu item while the other group sees the second item. However, the option value shown on the menu is the same.

User changes to menu options are propagated during an NLS upgrade. For user options, enter the same **Menu option** value that is specified in the **Official option** field.

### Descriptions

Specifies the short and long descriptions shown on the Menu panel. If you customize the descriptions, the values are propagated when an NLS upgrade is applied.

### Command (or MENU)

Specifies the command to run when a user selects the Menu item. This value can be a command (%CMD) or panel as normally specified in the ISPF panel body. To indicate that the Menu item opens a Menu when selected, specify **MENU xx**, where **xx** is the official option under which the menu items are defined. For example, **MENU SE** opens a menu that contains all the items with an Official option value of **SE xx**. **MENU SE D** shows a menu containing all the items with the Official option value **SE D**.

To open the next menu on a panel other than the main panel, specify the panel name in the field **Panel for "MENU"**. Except for the **LO** (local) option, user changes to the command field are *not* propagated during an NLS upgrade.

### Panel for "MENU"

Specifies the panel to open when a user selects the Menu option.

### New menu

If selected, add the Menu item to the Main menu. Use the following options to specify how the item is displayed:

**Y** to display the item on the Main menu.

**N** to display the item as expandable on the Main menu.

For expandable options, leave the **Panel for "MENU"** field blank and specify **MENU "option name"** in the **Command (or MENU)** field; for example, **MENU R@**.

## Customizing action line commands

In zSecure, you can configure the resources that determine which line commands are available on various panels. When the command runs, zSecure checks for READ access to the resource profile `$C2R.ACTION.xx.y.z`, where:

`xx` is the NEWLIST type.

`y` is the entity type.

`z` is the action.

You can customize the line commands in the following ways:

- Change the characters for running the command.
- Change the short or long description.
- Add or delete a line command.
- Customize the panel for the line command (Advanced users only).

To customize a line command, do the following steps:

1. From the Setup menu, type **SE.D** to display the Setup Defaults panel.
2. Type **N** to display the Setup - NLS panel.
3. In the **Action on language items** field, type **5 (Customize action line commands)**.
4. Press Enter to display the line command list panel shown in Figure 4.

```

zSecure - Setup - NLS (- SYSTEM DEFAULT ROW 33 OF 316
Command ==> Scroll ==> CSR
Specify action for menu item(s): Edit, Insert, Copy, Delete
Standard options Option and text as shown on panel
- RC D AC AC Access Access Check for one userid or group
- RC D C C Copy Copy data set profile
- RC D D D Delete Delete data set profile
- RC D E E Event Display event logging
- RC D L L List RACF listdsd command
- RC D LD LD List profile RACF listdsd DSNS command
- RC D LR LR List profile List datasets covered by profile
- RC D MI MI Instdata Manage data set instdata
- RC D MU MU Userdata Manage installation-defined USRDATA
- RC D R R Recreate Recreate data set profile
- RC D S S Select Show additional information
- RC D SE SE Segments Show application segments
- RC G A A Authorization Group authorization (permits and scope)
- RC G AC AC Access Show access for group
- RC G C C Copy Copy groupid
- RC G D D Delete Delete group

```

Figure 4. Setup NLS - Select line commands for customization

5. To work with a line command, type one of the following commands in the Line command selection field:
  - **E** to edit the settings for an existing menu item.
  - **I** to add a Line command.
  - **C** to copy a Line command entry as a template for creating an item.
  - **D** to delete a menu item.
6. Press Enter.
7. On the Line command specification panel, specify the line command settings. For more information, see “Line command specification panel” on page 17.
8. Press Enter to save the changes and return to the Line command list panel.
9. Repeat steps 5 - 8 for each line command you want to customize.
10. Press F3 to exit.
11. At the prompt, select one of the following options to process the changes:
  - N** applies the updated settings only to new users.
  - Y** applies the updated settings to all users when they log in.

The following list describes the options and fields available for customizing line commands:

**NEWLIST type**

Specifies the report type (NEWLIST) for which the line command is valid. You use a NEWLIST type template to select data and generate zSecure reports. Together with the entity type and action, the NEWLIST type determines the profile to check. In Figure 5 on page 18, the action settings apply to RACF reports (NEWLIST TYPE = RC).

### Entity type

Lists the entity type for which the line command is available; for example: USER, GROUP, or RESOURCE.

### Action

Specifies the action to run. You can view the actions defined in the product by scrolling through the line command list on the Setup - NLS panel shown in Figure 4 on page 16.

To add a new action command, include at least one of the following characters: @, #, or \$ in the Action name. These characters identify installation-defined action command. If the custom action name does not contain one of these characters, it is deleted when an NLS upgrade is applied.

### Specify Action for Menu item

Determines how to process the line command specification panel. Table 6 lists the available options.

Table 6. Actions available for selecting and customizing language and display options for line commands

Action	Description
1. Use as specified below	Applies the line command settings specified.
2. Delete menu item	Deletes the specified line command and exits the panel.
3. Reset all items to system defaults	Resets the line command to the system default descriptions and behavior. If no defaults have been specified, the default zSecure settings apply.
4. Reset to zSecure defaults	Resets the line command to the original product settings for the language specified.

### Used action

Specifies the line command available on the panels and shown in the action-pop-up panel. Changes to this field are propagated during an NLS upgrade.

### Description

Specifies the short and long description for the line command. The long description shows on the action-pop-up panel. Changes to these descriptions are propagated during an NLS upgrade.

**Panel** Specifies the panel to open when the action is specified. In the official zSecure panels, the variable &CKREREL. provides pull-down and non-pull-down panel functions. User changes to the panel field are *not* propagated during an NLS upgrade.

### Map CARLa fields into ISPF variables

Select this field to define a link between CARLa variables and ISPF variables. You must use CARLa-variables in query statements. Use ISPF-variables to show values on the specified panel.

### Line command specification panel

Figure 5 on page 18 shows the panel for customizing line command settings. This panel opens when you edit, copy, insert, or delete a line command on the Setup - NLS Line command list panel shown in Figure 4 on page 16.

```

zSecure - Setup - NLS (- SYSTEM DEFAULTS)
Command ==>
Newlist type . . . . RC          (i.e. RC for RACF)
Entity type . . . . U          (i.e. U for USER)
Action . . . . . C          (i.e. C for COPY)

Specify action for Menu item
1 1. Use as specified below      2. Delete Menu item
   3. Reset to system defaults    4. Reset to Security zSecure defaults

Used action . . . . C          (as displayed on user menu)
Short description . Copy
Long description . Copy userid
Panel . . . . . C2RP&CKREREL.UC@ (panel to use for action specification)

/ Map CARLa fields into ISPF variables

Press ENTER to continue.

```

Figure 5. Setup NLS options - Line command specification panel

The following list describes the options and fields available for customizing line commands:

**NEWLIST type**

Specifies the report type (NEWLIST) for which the line command is valid. You use a NEWLIST type template to select data and generate zSecure reports. Together with the entity type and action, the NEWLIST type determines the profile to check. In , the action settings apply to RACF reports (NEWLIST TYPE = RC).

**Entity type**

Lists the entity type for which the line command is available; for example: USER, GROUP, or RESOURCE.

**Action**

Specifies the action to run. You can view the actions defined in the product by scrolling through the line command list on the Setup - NLS panel shown in .

To add a new action command, include at least one of the following characters: @, #, or \$ in the Action name. These characters identify installation-defined action command. If the custom action name does not contain one of these characters, it is deleted when an NLS upgrade is applied.

**Specify Action for Menu item**

Determines how to process the line command specification panel. Table 7 lists the available options.

Table 7. Actions available for selecting and customizing language and display options for line commands

Action	Description
1. Use as specified below	Applies the line command settings specified.
2. Delete menu item	Deletes the specified line command and exits the panel.
3. Reset all items to system defaults	Resets the line command to the system default descriptions and behavior. If no defaults have been specified, the default zSecure settings apply.

Table 7. Actions available for selecting and customizing language and display options for line commands (continued)

Action	Description
4. Reset to zSecure defaults	Resets the line command to the original product settings for the language specified.

**Used action**

Specifies the line command available on the panels and shown in the action-pop-up panel. Changes to this field are propagated during an NLS upgrade.

**Description**

Specifies the short and long description for the line command. The long description shows on the action-pop-up panel. Changes to these descriptions are propagated during an NLS upgrade.

**Panel**

Specifies the panel to open when the action is specified. In the official zSecure panels, the variable &CKREREL. provides pull-down and non-pull-down panel functions. User changes to the panel field are *not* propagated during an NLS upgrade.

**Map CARLa fields into ISPF variables**

Select this field to define a link between CARLa variables and ISPF variables. You must use CARLa-variables in query statements. Use ISPF-variables to show values on the specified panel.

## Adding and selecting CARLa command libraries (SE.D.8)

Use the Setup Default - Command files option (SE.D.8) to specify the CARLa command libraries for the product. These CARLa command libraries contain scripts that perform zSecure functions. You can manage the scripts and run them from the **Setup Default - Command** file panel and also from the **Command (CO)** menu option.

zSecure provides the CKRCARLA library, which contains sample programs. This library is automatically included in the library definitions when you install the product.

Select the Setup Default - Command files option to display the Setup - Command file panel shown in Figure 6. Use this panel to manage the command libraries.

```

----- zSecure Manager for RACF select library with  ROW 1 OF 11
COMMAND ==>                                     SCROLL ==> CSR

Enter CMS Filename (fn ft fm). Type END or press PF3 when complete.
Valid line commands are S(select), E(edit), I(insert), R(repeat) and D(delete)

  CMS file pattern (e.g. * CARLA * or CKA* CARLA E)
*      CKACUST *                                     site
* CARLA *                                           default
***** BOTTOM OF DATA *****

```

Figure 6. Setup - Command file panel

You must specify a CMS filename (fn) filetype (ft) filemode (fm) or a pattern. Use the line commands described in Table 8 on page 20 to manage the library list and select libraries.

Table 8. Available Line Commands

Line command	Description
E	Lists the script files from the CMS mini disks.
D	Deletes the file (fn ft fm) from the selection list.
I	Adds a new line to the selection list for specifying the name of another member.
R	Copies an entry to a new line so that you can edit the CMS file name.
S	Makes the CMS file available to all zSecure users.

---

## Setting up rule-based compliance evaluations (option AU.R)

After installing the software, the AU.R sample customization files CKVG@IDF SAMPLE and CKVG@INS SAMPLE are available on the production build disk. You must copy these files to the minidisk specified with the CKACUSTMiniDisk parameter in C2R\$PARV CKVPARM as CKVG@IDF CKACUST and CKVG@INS CKACUST.



---

## Chapter 5. Making the software available in CMS

### About this task

Use the following procedure to make the installed software available to CMS users.

**Note:** If you are upgrading from a previous release of the product, see “Upgrading the product for CMS users.”

### Procedure

1. Copy the start program for the product to the minidisk for local tools or to another location that users have access to when they log on. The default start program, CKV, is a REXX program provided on the production build disk as CKV SAMPLE. CKV SAMPLE should be copied to CKV EXEC to your minidisk. You might need multiple copies of this program if you deploy the product on multiple z/VM images or require different configurations for different users. For information, see Setting up the configuration files.
2. For each program, review the following parameter settings and adjust them if necessary:

```
configurationFile      = 'C2R$PARV CKVPARAM *'  
codeMiniDisk          = '5655T13D 200'
```

#### **configurationFile**

Specifies the file (file name, file type, file mode) that configures zSecure Manager for RACF z/VM. See Configure the product.

You can override the configuration file at run time by specifying a configuration file name on the start command for the product. See “Selecting a configuration file” on page 7.

#### **codeMiniDisk**

Specifies the owner and device number of the minidisk for the installed software. The owner is a VM user ID. CodeMiniDisk must correspond to the VM Directory entry of the user ID that installed the product. Typically, the VM user ID is 5655T13D and the installed software is found on a production build minidisk with a device address of 200.

3. Establish the method to start the program in CMS. See Establish the start method for CMS users.

---

## Upgrading the product for CMS users

### About this task

If you are upgrading from a previous release, then you might have a customized copy of the start program: CKV or C2REVM, as it was previously named. You can continue using your customized start program with the new release. However, you must review the custom copy to determine whether it requires any updates.

To prepare to upgrade the product, do the following steps:

## Procedure

1. Examine the CKV SAMPLE program provided with the new software to determine whether it contains any new logic. If necessary, adapt your customized program to incorporate the changes.
2. If you install the new software on a different minidisk, update your version of the REXX start program to point to the new minidisk.
3. If necessary, adapt the procedures to start the product in CMS. See Establish the start method for CMS users.

---

## Establishing the start method for CMS users

You can use zSecure in several different modes.

### Full-screen mode

Using zSecure in full-screen mode requires ISPF.

- If you are already using ISPF for other products, you probably have a local menu that gives access to your ISPF applications. In that case, update this menu to include zSecure. The following example shows the menu entry for zSecure. The menu entry for RACF is also shown, as an example only:

```
/******  
/* MENU SHOWN TO USER */  
/******  
% R +RACF - Resource Access Control Facility  
% Z +ZSECURE - zSecure Manager for RACF z/VM  
%  
  
/******  
/* ACTION CHARACTER TRANSLATION */  
/******  
R, 'CMD(EXEC RACF ISPF) NEWAPPL(ICH)'  
Z, 'CMD(CKV)'  
, ' ', '  
, ' ', '  
X, 'EXIT'
```

- If you are not already using ISPF applications, you can have your users start zSecure from the CMS command line. zSecure starts ISPF, as long as the ISPFMiniDisk parameter in the zSecure configuration is correct. The command is:

```
CKV
```

Instead of CKV, you might want to substitute the name that you assigned to your local copy of the start program.

### Line mode

Running zSecure in line mode means that the ISPF Dialog Manager is not being used. When ISPF is not installed in your system, this mode is selected automatically. When ISPF is available, and you nevertheless want to use zSecure in line mode, use the following command:

```
CKV ( MODE=LINE
```

### Unattended

Production processes, like the daily refresh of the CKFREEZE and UNLOAD files, often run unattended; for example, in a userid that is XAUTOLOGged at regular intervals. Set up such a userid and create a PROFILE EXEC to directly call **CKVCOLL**, **CKRCARLA**, or both. For instructions, see the *IBM Security zSecure Manager for RACF z/VM: User Reference Manual*. Make sure that your PROFILE EXEC includes a **LOGOFF** command; otherwise the userid might remain active (although disconnected) and a subsequent XAUTOLOG will fail.

---

## Chapter 6. Setting up for production

Perform the following procedures to set up the product for production:

- “Capacity planning”
- Specify the default input set
- Set up the daily collection process
- Refresh the CKFREEZE file

---

### Capacity planning

The IBM Security zSecure Manager for RACF z/VM product consists of multiple components. The product provides functions for reporting about information in the security database, reporting about events that occurred in the system (SMF), and detailed analysis of the security environment. See the sections that follow for information about possible data set sizes, virtual storage needs, and CPU time requirements.

You can find planning information for the following types of system resources in this section:

- Direct access storage device (DASD) storage required for storing the data used or created by the program
- Virtual storage required for running the program
- CPU time used by the program

### DASD storage

Data storage on DASD (disk) as used by zSecure is mainly for the following types of data:

#### CKFREEZE

This type of file contains information about the system and resources. This includes many system control blocks and information about the system configuration. The CKFREEZE file is created by the zSecure CKVCOLL program. The information is used by other zSecure components. For daily zSecure usage, you need a CKFREEZE file for each system that you are managing.

In the z/VM environment, CKFREEZE files are created by the CKVCOLL program. In contrast to the CKFCOLL program on z/OS, the CKVCOLL program does not provide many options to specify the information collected. The CKVCOLL program collects information from RACF, the real device configuration, and certain virtual devices (mainly networking devices). It also extracts information from the specified USER DIRECT file. The size of the resulting CKFREEZE file mainly depends on the number of real devices present in the system and the number of users and minidisks defined in the USER DIRECT file.

As a rule, you can use the following amounts for the space required in the CKFREEZE file:

- 0.1 MB base size
- One third of the size of the USER DIRECT file
- 1 MB per 5000 defined real devices

In a formula:

$$\text{Size(MB)} = 0.1 + U/3 + D/5000$$

where:

U = size of the USER DIRECT file

D = number of defined real devices

The size of the USER DIRECT file as used in this calculation is the size in megabytes of the file when using 80-byte fixed-length records. If you use a different record format, or different line length, the size calculation must be adapted accordingly.

### **RACF Data**

zSecure Manager for RACF z/VM often needs information from a RACF source. This source can be an existing RACF database. No extracts or copies are required. You can also use a private backup copy of the RACF database. If you use a private backup copy, plan for DASD space equal to the size of your current database. You can also use a proprietary format UNLOAD copy of the RACF database. Such an UNLOAD file can be used as frozen input to generate reports. The size of an UNLOAD file is approximately the same as the used part of your database. The UNLOAD file has, as an additional advantage, that all sensitive fields like passwords have been removed from the UNLOAD copy.

### **SMF Data**

This data is not unique to zSecure. SMF records are created to provide information about the security environment and events in the system. They contain information that is useful for auditing purposes. Data is collected about many different types of events. zSecure Manager for RACF z/VM can use SMF data as input to report about historic events in the system. If you want to report about events for a certain period, the SMF data for that period must be available. The required data can be on tape or on DASD. For reporting about SMF events, processing of the SMF data sets is sequential. Therefore, multiple data sets with SMF records can be on the same tape.

## **Virtual storage**

Virtual storage is needed while running the program. The amount of virtual storage needed is dependent on the amount of data processed during the report or analysis. For most types of reports, the virtual storage needed is of the same order as the size of the output report. For example, if you are generating a report of 4,000,000 SMF records with detail information, the program needs sufficient space to retain all unique field values that occur in these records. Typical reports require up to 250 MB of virtual memory. You can significantly reduce virtual storage requirements by careful selection of the type of events, users, or resources to be included in the report.

## **CPU time**

The amount of CPU time used is the CPU time used by the user who is running the zSecure programs to create reports. The CPU time needed for creating interactive reports depends on the size of the data to be analyzed and the size of the resulting report. Typical reports take a few seconds to create. Large reports might take several minutes. Due to the amount of data, generating large SMF summary reports might take a significant amount of CPU time.

## Network load

Security zSecure Manager for RACF z/VM does not generate any significant network load.

---

## Specifying the default input set

For new users, update the following configuration parameters to specify a default input set containing the RACF database on an OS-formatted minidisk. These parameters are included in the default zSecure configuration file C2R\$PARV CKVPARM or the customized configuration file you created previously.

- **racfDbDataset**
- **racfMiniDisk**
- **racfFileMode**
- **racfVirtualAddress**

For more information, see the following topics:

- Set up the configuration files
- Appendix A, “Configuration parameters,” on page 31

---

## Setting up the daily collection process

The zSecure Collect program (CKVECOLL) collects the required data and writes it to a CKFREEZE file. This file is the input data source for RACF administration and auditing functions. Any user ID that collects this information must have CP privilege classes A, B, E, and G.

If the VMCMD DIAG0A0.RACONFIG profile is defined and active, then READ access to this profile is also required.

You can run the data collection process using any of the following methods:

- From the Setup - Input files menu, select the **Allocate new data sets for CKFREEZE** to set up the files and collect the data. Instructions are available on the panel and in the ISPF online help (F1).
- Run the command to start the program directly from CMS:  
CMS CKVECOLL <parameters> (<commands>)
- Run the REXX program CKVECOLL from a user ID that can log on using AUTOLOG or XAUTOLOG commands.

This method requires starting the program from the PROFILE EXEC. After starting the program, subsequent processing is required to archive or save the collected data.

If a user must collect statistics on a regular basis, use this method for the daily collection process.

For information about the CKVECOLL parameters and commands, see “Data collection parameters.”

## Data collection parameters

The following example shows the syntax to run the CKVECOLL program from CMS or from the PROFILE EXEC of a user ID that can log on with AUTOLOG or XAUTOLOG commands.

```
CKVECOLL <parameters> (<commands>)
```

You can specify optional input parameters for the CKVECOLL program to identify the system and VM Directory file for the input data source. When the program runs, it uses these values to search for the data source. If you do not supply either of these parameters, the program collects information and creates USER SYSPRINT and USER CKFREEZE files.

The following list describes the optional parameters. For examples using these parameters, see “Examples: Commands for collecting and storing data.”

**System name**

Optional. The system name specifies the system that is the source for the data collection. If you use this parameter, specify it before the VM directory file source parameter.

**VM directory file source**

Optional. The VM directory file source parameter specifies the directory source for the data. This parameter can have several formats:

**name** A single value is interpreted as a file name. The program assigns a default file type of DIRECT. When the program runs, it searches all available disks for the VM Directory file with the specified name.

**name type**

With two values, the first value is the file name; the second specifies the file type. When the program runs, it searches all available disks for the VM Directory file with the specified file name and file type.

**name type mode**

Three values are parsed as file name, file type, and file mode.

**Examples: Commands for collecting and storing data**

The following examples show the different methods to run the CKVECOLL program to collect data and store it in the VMASYS SYSPRINT and VMASYS CKFREEZE files.

**Collect data using the default VM system directory.**

When you run the following command, the directory information must be in the VMASYS DIRECT file. The data is written to USER VMASYS and USER CKFREEZE files.

```
ckveco11
```

**Collect data using a specified VM system directory**

When you run the following command, the directory information must be in VMASYS DIRECT. The data is written to the VMASYS SYSPRINT and VMASYS CKFREEZE files.

```
ckveco11 vmasys
```

**Collect information using a specified file**

When you run the following command, the directory information must be in the USER DIRECT file. The data is written to the VMASYS SYSPRINT and VMASYS CKFREEZE files.

```
ckveco11 vmasys user
```

**Collect information using a specified system and a VM directory called VMSYS BACKUP**

When you run the following command, the VM directory file information must be in the VMSYS BACKUP file. The data is written to the VMASYS SYSPRINT and VMASYS CKFREEZE files.

```
ckveco11 vmasys vmsys backup
```

### **Collect information from a specified system from the file with the specified file name, file type, and mode**

When you run the following command, the directory information must be in the USER BACKUP M file. This command specifies a specific data source that does not require searching the available disks for the VM directory file. The data is written to the VMASYS SYSPRINT and VMASYS CKFREEZE files.

```
ckvecoll vmasys user backup m
```

---

## **Refreshing the CKFREEZE file**

### **About this task**

All Audit functions and many Admin functions require a CKFREEZE file that contains the collected system data. After you create the initial CKFREEZE file, use the REFRESH transaction from the Setup files panel to refresh the data at regular intervals. For information about creating the CKFREEZE and collecting data, see Set up for production and Set up the daily collection process.

1. From the product menu, type **SE.1** on the command line to display the Setup - Input Files panel.
2. Run the **F** line command to refresh the CKFREEZE file.
3. Press Enter to generate the new CKFREEZE file.





---

## Chapter 7. Verifying the installation

Before notifying users that the software is available, run the following checks to confirm that the software was installed and configured correctly.

- Check the base UI functions
- Check the zSecure Collect function
- Check installation-defined option settings for CKGRACF operations

---

### Checking the base UI functions

#### About this task

Verify that the primary menu and menu options operate correctly:

1. To verify that the primary menu works, start the program from the ISPF panel selection or from the CMS command line. See *Make the software available to CMS users*.

#### Example run command for customized configuration file

```
CMS CKV (CONFIG = MYCONFIG configfiletype x)
```

2. If the product does not start in ISPF, take the following actions:
  - Verify the location and name of the configuration file.
  - Review the settings to verify that the product is configured correctly. (See *Configure the product*.)
3. From the Main Menu, select several options to make sure that the panels open correctly and have the expected content.

To customize the product panels, see *Customize options for user groups*

---

### Checking the zSecure Collect function

#### About this task

Verify that the zSecure Collect function collects data:

#### Procedure

1. Log on with a user ID that has privilege classes B, E, and G.
2. Confirm that the user ID has at least read access to the minidisk where the VM directory file is stored, or a copy of the VM Directory file.
3. From the zSecure Manager for RACF z/VM main menu, type **SE.1** (Setup files) on the command line.
4. Remove the selection entry from all selected input sets.
5. Create a CKFREEZE file:
  - a. Type **SE.2** on the command line at the top of the main menu to display the Setup - New files panel.
  - b. When prompted, specify the allocation parameters for the CKFREEZE file. Allocate 2 MB for each online DASD-volume.
6. To collect and write data to the files, run the REFRESH command from the **SE.1** menu option.
7. Browse the newly allocated CKFREEZE file to verify that it contains the expected data.

---

## Checking installation-defined option settings

### About this task

The optional CKRSITE load library contains any installation-defined values for zSecure installation settings. See *Customize installation options* .

If a CKRSITE load library exists, verify that it works and that the reported values match those values specified in the CKRSITE ASSEMBLE code for building the library.

1. Start the product in line mode:

```
CKV ( MODE = LINE
```

where CKV is the name of the REXX program that starts the product.

2. Type **SHOW CKRSITE** to show the installation-defined values for the installation settings.
3. Press Enter three times.
4. Examine the SYSPRINT for the portion showing the installation settings.

The following code samples show the default values.

```
CKR0009 00 No customer/site specific name to be used as default CHECKPWD
          Running under CMS
          CPU-id
          Product codes MANAGERVM
          5655-T13 IBM Security zSecure Manager for RACF z/VM
```

```
CKR0525 00 Contents of CKRSITE module:
          Class:           XFACILIT
          Authority:       SINGLE
          Force restrict:   N
```

5. Check that the reported values match the values specified in the CKRSITE ASSEMBLE code.

---

## Appendix A. Configuration parameters

The Configuration parameters define the location of the software and other resources required to run the product. These parameters are specified in the configuration file described in the Chapter 2, “Installation overview,” on page 3. Several of the configuration parameters use the *file mode* setting. The CMS ACCESS command also uses this setting. Starting the product establishes the access for the minidisk where the software is stored. See Make the software available to CMS users. For all other file modes that are specified in the configuration, you must set up the appropriate LINK and ACCESS commands in advance. This configuration is not required for files stored on the same minidisk as the software.

You can also code parameters that are listed for the configuration as overrides. The following example shows the command to start the product with an override for the configuration file.

```
CKV (CONFIG = MYCONFIG C2RPARM A
```

The following example shows a Start command that overrides the CUSTOMIZATIONFILEMODE specified in the configuration file.

```
CKV (CUSTOMIZATIONFILEMODE = ''
```

The following list describes the configuration parameters:

### **CKACUSTMiniDisk**

Specifies the minidisk location of the CKACUST files. (See “Setting up rule-based compliance evaluations (option AU.R)” on page 20.) This minidisk is linked during UI startup. Specify the value as: *userid minidisk*, where the values match the VM directory that defines the minidisk under its owner. The rule-based compliance checking (AU.R) uses CKACUST files on this disk. To maintain these files, a user must have UPDATE access to this disk; otherwise, READ access is required. For more information about the AU.R option, see the *IBM Security zSecure Manager for RACF z/VM: User Reference Manual*.

### **customizationFileMode**

Specifies the file mode to access the minidisk location for configuration files and any SETUP DEFAULT option files created to customize the ISPF interface. If your site uses Setup Default options, specify a file mode that permits update access to the minidisk. Otherwise, read access is sufficient.

If minidisk location cannot be linked and accessed using the specified file mode when the product starts, you can start the program from the ISPF interface. Starting the program from ISPF can prevent users from inadvertently working with incorrect configuration settings like the wrong input file set.

**Note:** SETUP DEFAULT option files have *file type* C2RPROF. If no SETUP DEFAULT files are available, they are disabled. You can create them using the SETUP DEFAULT options described in Customize options for user groups.

### **description, ckfreeze, smf, unload**

Describes a set of input files available to all users of this configuration. When you specify a *description*, you also must specify the correct CKFREEZE, SMF, or unload input file source.

For example, you can specify the following values in the *description*, *ckfreeze*, and *smf* fields:

```
description      = 'Default set'
ckfreeze         = 'DAILY CKFREEZE D'
smf              = 'DAILY SMF D'
```

Based on these values, zSecure Manager for RACF z/VM uses the indicated CKFREEZE and SMF files. When running in line mode, FILEDEFS are generated for these input files.

These input files provide the default input source when the option to use the last input source is not enabled for a user ID. Use the Setup Default option to change the setting that specifies what values to use when the product starts.

#### **earlyWrn**

A list of user IDs that are to receive messages when unsupported or obsolete parameters are found in the configuration member. If you specify multiple user IDs, separate them with commas and put them between single quotation marks; for example, 'ADMIN1,ADMIN2,ADMIN3'. If this parameter is left empty, all users receive these messages.

**init** Indicates the parameter values the program uses when it starts. You can specify either of the following values:

**YES/RESET** reset all parameters to their defaults. The parameter values can be system defaults, or the values that have been set from the Setup Default (**SE.D**) option.

**NO** Use the parameter values from the last session for the user ID.

#### **ISPFMiniDisk**

Specifies the minidisk location of the ISPF code. Specify the value as: *userid minidisk*, where the values match the VM directory that defines the minidisk under its owner. When **CKV** is called with **MODE=ISPF** or **MODE=ISPFPDF** and the ISPF code is not found, this disk is linked and accessed.

**mode** Represents the mode that the product is in when it is started by the CKV REXX program. The mode value can be **LINE**, **ISPF**, or **ISPFPDF**.

If the mode parameter is not set and ISPF is available, ISPF is used. If the mode parameter is not set and ISPF is not available, LINE is used.

LINE starts the product in a data entry session, ready to receive CARLa commands.

ISPF starts the product at the Main Menu. CMS XEDIT and BROWSE functions are used.

ISPFPDF starts the product at the Main Menu. ISPF/PDF EDIT and BROWSE functions are used.

**Note:** ISPF/PDF for VM/SP (5684-123) is not supported as of 1998.

#### **racfDbDataset**

Specifies the data set name of the RACF database stored on an operating-system-formatted minidisk. This data set provides the default input set and provides the input set for transaction SE.VM from the REXX program CKVECOPY. See Specify the default input set.

On z/VM 6.2 and higher, you can leave this parameter blank to set the active RACF backup database as the default for new users.

**Note:** The active RACF database requires access to security resource VMCMD DIAG0A0.RACONFIG.

**racfDBCMS**

Identifies the file name, file type, and file mode for the copy of the RACF data base in CMS format. This file receives the data generated by transaction SE.VM from the REXX program CKVECOPY.

**racfFileMode**

Specifies the *File mode* to access the *racfDbDataset*. You can specify *freemode* to automatically deduce a file mode if you have the ISPF product installed. This file mode is used for selecting the default input set. See Specify the default input set.

**racfMiniDisk**

Specifies the mini disk location of the RACF database copy that you specified in *racfDbDataset*. Specify the value as: *userid minidisk* where the values match the VM directory that defines the minidisk under its owner. This minidisk is checked when the default input set is selected. See Specify the default input set.

**racfVirtualAddress**

Specifies the virtual address to access the RACF database copy specified in the *racfDbDataset* parameter. You can specify *freeaddr* to automatically deduce a virtual address if you have the ISPF product installed. This address is checked when the default input set is selected. See Specify the default input set.

**userLibFileMode**

Can be specified to indicate installation or user-specific zSecure modules that must be used in addition to the common modules. The ISPF interface searches for additional modules. If the modules exist, they are concatenated in front of the corresponding zSecure common modules. The module types searched for are PANEL, MSG, SKELETON, and TABLE.

**workFileMode**

Allocates the work files created by the ISPF interface.



---

## Appendix B. Setting up and starting a CMSBATCH server

For the CO.5 submit function, a CMSBATCH server (or other batch facility) is required. The CMSBATCH feature is a standard component of z/VM, but it must be set up for z/Secure usage and especially to be protected from unauthorized usage.

To set up and start a CMSBATCH server, use the following steps:

1. Define a new userid like the following sample directory:

```
USER CKVBATCH AUTOONLY 256M 512M ABEG
  INCLUDE IBMDFLT
  IPL CMS PARM BATCH
  MDISK 0195 3390 XXXX 0150 XXXXXX M
```

2. Define the RACF profiles:

```
RAC ADDUSER CKVBATCH NAME('ZSECURE BATCH') NOPASSWORD NOPHRASE OWNER(IBMUSER) DFLTGRP(SYS1)
RAC RDEFINE VMMDISK CKVBATCH.195 UACC(NONE) OWNER(IBMUSER)
RAC PERMIT CKVBATCH.195 CLASS(VMMDISK) RESET ID(CKVBATCH) ACCESS(CONTROL)
RAC RDEFINE VMRDR CKVBATCH UACC(NONE) OWNER(IBMUSER)
RAC PERMIT CKVBATCH CLASS(VMRDR) RESET
```

3. Grant the batch server access to the code disk and the RACF database:

```
RAC PERMIT 5655T13D.200 CLASS(VMMDISK) ID(CKVBATCH)
RAC PERMIT RACFVM.200 CLASS(VMMDISK) ID(CKVBATCH)
```

4. Grant authority for the Diagnose 0A0, subcode 0050 function.

If the VMCMD DIAG0A0.RACONFIG profile has been defined to protect the Diagnose 0A0, subcode 0050 function, then you must grant the batch server read access to this profile. Otherwise CP classes A, B, or both, are sufficient for this function.

```
RAC PERMIT DIAG0A0.RACONFIG CLASS(VMCMD) ID(CKVBATCH)
```

5. Grant each userid that needs to use the batch service access to the VMRDR CKVBATCH profile, and grant the batch server read access to the user A-disks:

```
RAC PERMIT CKVBATCH CLASS(VMRDR) ACCESS(UPDATE) ID(ckv_user)
RAC PERMIT ckv_user.191 CLASS(VMMDISK) ID(CKVBATCH)
```

To prevent remote users from submitting jobs through RSCS or SMTP, they must *not* have a matching VMXEVENT USERSEL.*server* profile that excludes the TRANSFER.D or TRANSFER.G commands from RACF control. A remote or local user who has such a profile can potentially submit jobs through these network servers and bypass the access controls. Bypassing the access controls makes it possible for the user to, for example, shut down the system or attach devices.

6. To start the server, add the server to the list of userids started by the PROFILE EXEC on the AUTOLOG2 0191 disk to make sure that it gets started immediately after a system IPL. If you have a monitoring service (for example, IBM Operations Manager), then you can also add the CKVBATCH server as a monitored service machine.





---

## Appendix C. 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.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

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.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

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

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

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

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. \_enter the year or years\_. All rights reserved.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://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](http://www.ibm.com/legal/copytrade.shtml).

Adobe, the Adobe logo, Acrobat, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

Other company, product, and service names may be trademarks or service marks of others.



---

# Index

## A

accessibility ix  
AU.R 20

## C

C2\$PARV SAMPLE 3  
capacity planning 23  
CKACUSTMiniDisk  
    configuration parameter under  
        VM/CMS 31  
ckfreeze  
    configuration parameter under  
        VM/CMS 31  
CKRCARLA library  
    sample programs 19  
CKRSITE load library  
    build 9  
    verify 30  
CKRSITE module  
    custom CKRSITE load library 8, 9  
    parameters 8, 9  
CKV 3  
CMS users  
    making zSecure software  
        available 21  
CMSBATCH server setup 35  
commands  
    CO 19  
    Define available 19  
    edit script 19  
    Run 19  
    specify library for 19  
configuration  
    define the configuration file 21  
    establishing initial 21  
configuration data sets 5  
configuration file  
    default 3  
    definition of 3  
configuration parameter under VM/CMS  
    CKACUSTMiniDisk 31  
    ckfreeze 31  
    customizationFileMode 31  
    description 31  
    earlyWrn 32  
    init. 32  
    ISPFMiniDisk 32  
    mode 32  
    racfDBCMS 33  
    racfDbDataset 32  
    racfFileMode 33  
    racfMiniDisk 33  
    racfVirtualAddress 33  
    smf 31  
    unload 31  
    userLibFileMode 33  
    workFileMode 33  
configuration parameters  
    codeMiniDisk 21

configuration parameters (*continued*)  
    configurationFile 21  
configuring 7  
    customizing configuration settings 7  
    default settings 7  
    setting up the configuration files 7  
CRMBATCH 35  
customizationFileMode  
    configuration parameter under  
        VM/CMS 31  
customize  
    options for user groups 10  
    using the Setup Default options 10  
    verifying option settings 10

## D

default  
    line commands 15  
    menu items 13  
    user options 10  
    User-defined settings 10  
    zSecure settings 10  
default configuration  
    C2R\$PARV CKVPARM 7  
default Start program 3  
description  
    configuration parameter under  
        VM/CMS 31  
distribution-oriented install  
    configuration data sets 5  
donfiguring  
    selecting a configuration file 7

## E

earlyWrn  
    configuration parameter under  
        VM/CMS 32  
education ix

## F

fresh CKFREEZE  
    fresh UNLOAD 27

## I

IBM  
    Software Support x  
    Support Assistant x  
init  
    configuration parameter under  
        VM/CMS 32  
installation  
    preparing for 5  
installation options  
    c 8  
    command timeout 8

installation options (*continued*)  
    customizing 8  
    default 8  
    multi-authority setting 8  
    resource class for security checks 8  
    timeout for saving completed  
        commands and scheduled actions 8  
installation-defined settings  
    default settings 8  
installing with VMSES/E  
    evaluating space requirements 5  
ISPFMiniDisk  
    configuration parameter under  
        VM/CMS 32

## L

line commands  
    customize 15

## M

menu  
    adding an installation-defined  
        option 14  
menus  
    customize 13  
minidisks  
    accessing configuration data from 3  
    storing configuration data 3  
mode  
    configuration parameter under  
        VM/CMS 32

## N

National Language Support (NLS)  
    Customize Line commands 15  
    Customize Menu items 13  
    customizing settings for 11  
    installation-defined names for  
        selection options 11

## O

online  
    publications v  
    terminology v

## P

problem-determination x  
Program directory  
    accessing 5  
    space requirements 5  
publications  
    accessing online v  
    list of for this product v

## R

- racfDBCMS
  - configuration parameter under VM/CMS 33
- racfDbDataset
  - configuration parameter under VM/CMS 32
- racfFileMode
  - configuration parameter under VM/CMS 33
- racfMiniDisk
  - configuration parameter under VM/CMS 33
- racfVirtualAddress
  - configuration parameter under VM/CMS 33
- release
  - verifying the release number 5
- resources required 23
- REXX program
  - C2REVM 21
  - CKV 21
- rule-based compliance evaluations 20

## S

- script library
  - Add 19
  - in CARLa language 19
  - Select 19
- SE.D 10
- selection options
  - customizing the option names 11
- Setup
  - NLS panel 12
  - SE.D option 12
- Setup - NLS panel
  - Line command list 16
  - Line command specification 17
  - Menu item list 13
  - Menu item specification 14
- Setup Default
  - National Language Support (NLS) 11
    - line command settings 15
    - Menu item settings 13
- Setup Default option (SE.D) 10
- site module
  - default settings 8
- smf
  - configuration parameter under VM/CMS 31
- Start program
  - CKV 21
  - copy 21
  - create multiple versions 21
- system resources 23

## T

- terminology v
- training ix
- troubleshooting x

## U

- unload
  - configuration parameter under VM/CMS 31
- upgrading the product
  - C2REVM 21
  - CKV 21
- userLibFileMode
  - configuration parameter under VM/CMS 33

## V

- verifying the installation
  - checking the base UI functions 29
  - checking the zSecure Collect function 29

## W

- workFileMode
  - configuration parameter under VM/CMS 33

## X

- XFACILIT 8

## Z

- zSecure Manager for RACF z/VM
  - making software available for CMS users 21





Printed in USA

SC27-4363-01

