

Adabas Encryption for z/OS

Reference

Version 8.5.1

October 2021

This document applies to Adabas Encryption for z/OS Version 8.5.1 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2021 Software AG, Darmstadt, Germany and/or Software AG USA, Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses/> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third-Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software AG.

Document ID: EZ-REFERENCE-851-20210730EN

Table of Contents

Reference	v
1 About this Documentation	1
Document Conventions	2
Online Information and Support	2
Data Protection	3
2 Messages and Codes	5
ADAI* - ADAIOR System Messages	6
ADARUN Statement/Parameter Messages	8
User Abend Code	8
3 Glossary	9

Reference

This section provides reference information relating to the use of Adabas Encryption.

Messages and Codes	Describes the new and changed messages and codes generated by Adabas Encryption.
Glossary	Lists and defines terms.

1

About this Documentation

■ Document Conventions	2
■ Online Information and Support	2
■ Data Protection	3

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
Monospace font	Identifies service names and locations in the format <i>folder.subfolder.service</i> , APIs, Java classes, methods, properties.
<i>Italic</i>	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
Monospace font	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the symbol.
[]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at <https://documentation.softwareag.com>.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at <https://empower.softwareag.com/>.

You can find product information on the Software AG Empower Product Support website at <https://empower.softwareag.com>.

To submit feature/enhancement requests, get information about product availability, and download products, go to [Products](#).

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the [Knowledge Center](#).

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at https://empower.softwareag.com/public_directory.aspx and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at <https://techcommunity.softwareag.com>. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

2 Messages and Codes

■ ADAI* - ADAIOR System Messages	6
■ ADARUN Statement/Parameter Messages	8
■ User Abend Code	8

This section describes the new and changed messages and codes generated by Adabas Encryption. For all other error messages refer to the Adabas messages documentation.

ADAI* - ADAIOR System Messages

Adabas Encryption introduces the following new ADAIOR system messages.

ADAI36	No space for secondary extent on first volume of {ddname} Use non-zero primary space allocation for SPACE parameter in JCL DD statement and rerun the job
Explanation	<p>This message may be issued by ADAFRM when a new dataset is being formatted.</p> <p>There is no available space on the volume selected by z/OS for allocating the first secondary extent.</p> <p>Following this message, the job will be terminated with user abend 692.</p>
Action	<p>Specify non-zero primary allocations for the new datasets being formatted and rerun the job.</p>
ADAI37	Encryption buffer pool full
Explanation	<p>An attempt to allocate a buffer for encryption services has failed because there is no available space in the encryption buffer pool.</p> <p>The job will continue to run but performance may be severely degraded.</p>
Action	<p>Contact your Software AG support representative for information on how to tailor the encryption buffer pool size for your installation.</p>
ADAI45	{ddname }Open failed - {encryption support not available encryption support not available. Insufficient storage encryption support not available. Insufficient 64-bit storage encryption support not compatible with dataset type}
Explanation	<p>Refer to the table below for description and action:</p>

Message Ending	Description	Action
'encryption support not available'	An attempt was made to open an encrypted dataset, but the required support is not available.	<p>Ensure that ADARUN parameter ENCRYPTION=YES is specified and that a valid license for the Adabas encryption product has been processed successfully.</p> <p>If not, correct the error and rerun the job.</p>

Message Ending	Description	Action
		If the problem persists, contact your Software AG support representative.
'encryption support not available. Insufficient storage'	An attempt was made to open an encrypted dataset, but insufficient storage was available for the encryption parameter area.	Increase the REGION size and rerun the job. If the problem persists, contact your Software AG support representative.
'encryption support not available. Insufficient 64-bit storage'	An attempt was made to open an encrypted dataset, but insufficient storage was available for the encryption buffer area.	Ensure that the MEMLIMIT size permits an allocation of 16 MB above the 2 GB bar. If the problem persists, contact your Software AG support representative.
'encryption support not compatible with dataset type'	An attempt was made to open an encrypted dataset that is not compatible with the Adabas Encryption product.	Ensure that the encrypted dataset was formatted correctly using ADAFRM, with the key label specified on the JCL DD statement (DSKEYLBL) or derived from RACF or SMS. If the problem persists, contact your Software AG support representative.

Action See table above.

ADAI47 {ddname} {read | write | read GCB} encryption error
Return code {retcode} reason code {rsncode} | Parameter build error

Explanation Either the encryption service has returned an error indicated by the return code and reason code, or the encryption parameter list could not be built.

Action Contact your Software AG support representative.

ADAI81 Unable to complete increase of {ddname} – extent error

Explanation When Adabas Cluster Services or Adabas Parallel Services is being used, a request to increase the size of ASSO or DATA in a peer nucleus has not been able to process the new extent information correctly.

This might occur if, for example, additional volumes have been added to the dataset since the nuclei were started.

Action If new volumes have been added to the dataset since the nuclei were started, the increase will not complete until all participating nuclei are recycled.

If the problem persists, contact your Software AG support representative.

Adabas Encryption amends the following existing ADAIOR system message:

ADAI64	{dbid} {File {ddname} Dataset {dsn}} is being opened in mode {mode} Block size {blksize} RABN range {start-RABN} to {end-RABN} {File {ddname} Dataset {dsn}} is encrypted
Explanation	<p>The file (<i>ddname</i>) or dynamically allocated data set (<i>dsn</i>) is being opened in the mode (<i>mode</i>) given in the message (CKD, ECKD or zHPF). The file resides on a storage control device that supports count key data (CKD), extended count key data (ECKD) or high performance FICON (zHPF) channel commands. Adabas generates channel programs accordingly.</p> <p>The block size (<i>blksize</i>) of the data set is given in the message. It contains the blocks with numbers <i>start-RABN</i> through <i>end-RABN</i>.</p> <p>If the dataset is encrypted, an additional message line is generated to indicate this.</p>
Action	No action is required for this informational message.

ADARUN Statement/Parameter Messages

Adabas Encryption introduces the following new ADARUN error message:

Error-29	Loaded modules do not support ENCRYPTION
Explanation	The Adabas load library is not correct and does not fully support Adabas Encryption, Adabas Auditing or Adabas SAF Security 8.3. Either the ADAIOR/IOS modules do not support Adabas Encryption or some of the required maintenance in the nucleus and utilities is missing.
Action	Review and correct the JOBLIB/STEPLIB concatenation or combined load library, as per the installation instructions for Adabas Encryption. Ensure that all zaps required for Adabas Encryption, Adabas Auditing or Adabas SAF Security 8.3 have been applied.

User Abend Code

Adabas Encryption introduces the following new user abend code. It can be referred to in messages either in decimal notation (for example, 'U0692') or in hexadecimal notation (for example, x'2B4').

Code	Module	Explanation
692	ADAIOS	Dataset allocation error

3 Glossary

Acronym	Term	Description
AES	Advanced Encryption Standard	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
	Basic format sequential dataset	A sequential dataset in the original physical format, which can occupy up to 65,535 tracks on each volume
CPACF	Central Processor Assist for Cryptographic Function	A set of cryptographic instructions available in hardware on every zSeries processor unit
	Clear key	An encryption key whose clear, unconcealed value exists in memory, outside protected hardware (for example, Crypto Express), while it is being used to encrypt or decrypt data
	Crypto Express	A family of hardware security modules from IBM for high-security processing and cryptographic operations
	Cryptography	The practice and study of techniques for secure communication in the presence of adversaries
DASD	Direct-Access Storage Device	A device providing persistent storage in which each block (the smallest unit of an I/O operation) can be accessed directly and quickly by specifying its location on the device; colloquially also referred to as “disk”
DFSMS	Data Facility Storage Management Subsystem	A z/OS subsystem that automates and centralizes the management of persistent storage (disks and tapes)
	Encryption key	A parameter for an cryptographic algorithm. Must be kept secret in most applications (“secret key”), but some also work with “public keys”
EXCP	Execute Channel Program	A low-level I/O interface
	Extended format sequential dataset	A sequential dataset that can be striped, encrypted or compressed, or any combination thereof
ICSF	Integrated Cryptographic Service Facility	A z/OS subsystem that creates and manages cryptographic keys and performs crypto operations in software or hardware

Acronym	Term	Description
JCL	Job Control Language	The language of job control statements used to specify jobs to the job entry subsystem (JES)
JES	Job Entry Subsystem	A subsystem used by z/OS to receive jobs into the operating system, schedule jobs for processing, and control job output processing
	Key	In the context of encryption, a shorthand for encryption key
	Key label	A parameter to identify an encryption key, used by ICSF as a handle to locate the encryption key and its associated parameters
	Large format sequential dataset	A sequential dataset in an advanced physical format, which can occupy up to 16,777,215 tracks on each volume
	Protected key	A variation of secure key for high-performance bulk encryption and decryption using the CPACF instructions
RACF	Resource Access Control Facility	A component of the Security Server for z/OS, used to identify and authenticate users, authorize users to access protected resources, and record and report access attempts
	Secure key	An encryption key that has been encrypted under another key and is used in a way that its clear value never leaves a hardware security module (for example, Crypto Express)
SMS	Storage Management Subsystem	A shorthand for DFSMS, Data Facility Storage Management Subsystem
XTS	XOR-Encrypt-XOR Tweakable Block Cipher with Ciphertext Stealing	A block cipher mode of operation used for encrypting data on storage devices