

Adabas Encryption for z/OS

Reference

Version 8.6.1

September 2025

This document applies to Adabas Encryption for z/OS Version 8.6.1 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 © 2021-2025 Software GmbH, Darmstadt, Germany and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software GmbH product names are either trademarks or registered trademarks of Software GmbH 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 GmbH and/or its subsidiaries is located at <https://softwareag.com/licenses>.

Use of this software is subject to adherence to Software GmbH's licensing conditions and terms. These terms are part of the product documentation, located at <https://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 GmbH Products / Copyright and Trademark Notices of Software GmbH Products". These documents are part of the product documentation, located at <https://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 GmbH.

Document ID: EZ-REFERENCE-861-20250929EN

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
3 Glossary	7

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

Product Documentation

You can find the product documentation on our documentation website at <https://documentation.softwareag.com>.

Product Training

You can find helpful product training material on our Learning Portal at <https://learn.software-ag.com>.

Tech Community

You can collaborate with Software GmbH experts on our Tech Community website at <https://tech-community.softwareag.com>. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software GmbH news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories at <https://github.com/softwareag> and <https://hub.docker.com/publishers/softwareag> and discover additional Software GmbH resources.

Product Support

Support for Software GmbH products is provided to licensed customers via our Empower Portal at <https://empower.softwareag.com>. Many services on this portal require that you have an account. If you do not yet have one, you can request it at <https://empower.softwareag.com/register>. Once you have an account, you can, for example:

- Download products, updates and fixes.
- Search the Knowledge Center for technical information and tips.
- Subscribe to early warnings and critical alerts.
- Open and update support incidents.
- Add product feature requests.

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

For messages and codes generated by Adabas Encryption, refer to the Adabas messages documentation.

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