

# **Adabas SAF Security**

## **An Introduction to Adabas SAF Security**

Version 8.3.1

October 2021

This document applies to Adabas SAF Security Version 8.3.1 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: AAF-INTRO-831-20210928**

**Table of Contents**

- 1 About this Documentation ..... 1
  - Document Conventions ..... 2
  - Online Information and Support ..... 2
  - Data Protection ..... 3
- 2 An Introduction to Adabas SAF Security ..... 5
  - Benefits and Features ..... 6
  - Resource Protection ..... 6
  - Components ..... 8



# 1

## About this Documentation

---

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

## Document Conventions

---

Convention	Description
<b>Bold</b>	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](mailto: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](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      An Introduction to Adabas SAF Security

---

■ Benefits and Features .....	6
■ Resource Protection .....	6
■ Components .....	8

This document provides an introduction to Adabas SAF Security (ADASAF).

## Benefits and Features

---

The System Authorization Facility (SAF) is used by z/OS and compatible sites to provide rigorous control of the resources available to a user or group of users. Security packages such as RACF, CA-ACF2, and CA-Top Secret allow the system administrator:

- to maintain user identification credentials such as User ID and password; and
- to establish profiles determining the datasets, storage volumes, transactions, and reports available to a user.

The resulting security repository and the infrastructure to administer it represent a significant investment. At the same time, the volume of critical information held by a business is constantly growing, as is the number of users referencing the data. The challenge of controlling these ever-increasing accesses requires a solution that is flexible, easy to implement and, above all, one that safeguards the company's investment.

Adabas SAF Security (ADASAF) enhances the scope of SAF-based security packages by integrating Adabas resources into the central security repository. ADASAF enables

- a single control and audit system for all resources;
- industry-standard protection of Adabas data;
- maximized return on investment in the security repository.

## Resource Protection

---

Adabas SAF Security can be used to protect the following resources:

- [Adabas Resources](#)
- [COR-based Add-ons Online Administration Resources](#)

■ [Entire Net-Work Resources](#)

## Adabas Resources

Adabas SAF Security can be used to protect the following Adabas resources:

Resource	Protection
Adabas Nucleus	Only authorized users are allowed to: <ul style="list-style-type: none"> <li>■ start an Adabas nucleus</li> <li>■ perform Adabas nucleus administration functions</li> </ul>
Adabas Utilities	Only authorized users are allowed to execute utilities, and then only the appropriate ones. Authorization can be restricted by utility name/function/file as well as Database ID. For example, a user or group of users might be permitted to run ADAREP but not ADASAV against a particular database.
Database Files	Users or groups of users can be permitted (or denied) access to the basic resource of database files.
Database Commands	Access (READ/FIND) and update (STORE/UPDATE/DELETE) privileges can be granted to specific users or groups of users. To optimize performance, ADASAF disregards commands such as RC that are not file-specific.
Production Environment Data	Distinction can be made between a user operating in a production system and the same user operating in a test environment. This is known as cross-level checking and could be used, for example, to prevent damage by an application program inadvertently cataloged against the wrong Database ID.
Transaction Data	ADASAF can optionally validate requests to store or retrieve ET data.
Adabas Operator Commands	Restrictions can be placed on Adabas operator commands that can be issued from the MVS console.
File Passwords and Cipher Codes	Passwords and codes can be held in the security repository or supplied by a user exit and dynamically applied by ADASAF. This eliminates the need for the application to manage security data and removes the requirement to transmit sensitive information from the client to the database.
Adabas Basic Services	Adabas Basic Services can be protected with ADASAF by selecting the level of protection required (main functions only or main functions and subfunctions) and defining the appropriate resource profiles and granting the necessary users access to those profiles.
Stored Procedures	Only authorized users are allowed to invoke stored procedures.

This protection is provided by running Adabas SAF Security in the Adabas nucleus and utilities.

## COR-based Add-ons Online Administration Resources

Adabas SAF Security can be used to protect the online administration resources of the following COR-based Add-on products:

- Adabas SAF Security (SYSAAF)
- Adabas Fastpath (SYSAFP)
- Adabas Transaction Manager (SYSATM)
- Adabas Vista (SYSAVI)
- Adabas System Coordinator (SYSCOR)

This protection is provided by running Adabas SAF Security in the Adabas System Coordinator daemon.

## Entire Net-Work Resources

Adabas SAF Security can be used to protect the following Entire Net-Work resources:

Resource	Protection
Entire Net-work	Only authorized users are allowed to: <ul style="list-style-type: none"><li>■ start an Entire Net-Work job</li><li>■ perform Entire Net-Work administration functions</li></ul>

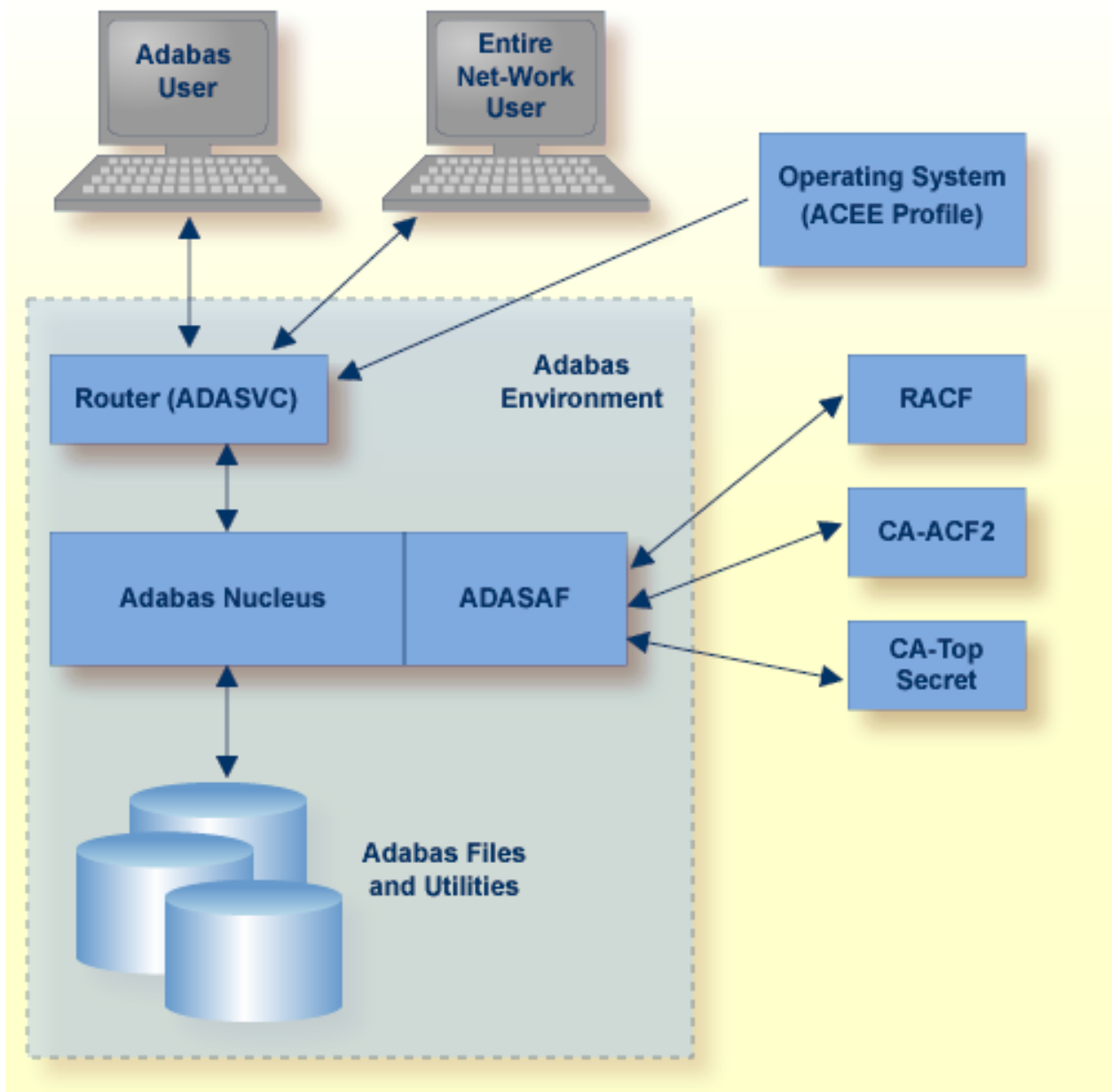
This protection is provided by running Adabas SAF Security under Entire Net-Work.

## Components

---

Adabas SAF Security runs in the address space of the job whose resources it is protecting.

The graphic below shows an example of the ADASAF main module running under an Adabas nucleus.



All users must first log on to their system using their Logon ID, usually a user name or code. Through the operating system or TP monitor, the installed security package performs authentication checks using the user's supplied Logon ID and password.

When access is from a remote workstation or non-IBM platform, the Logon ID and logon password must be given to Adabas SAF Security using a remote logon procedure, as described in the section *Logging On to a Database*.

For Adabas, the router extracts the user's Logon ID from the system ACEE and makes it available in the Adabas nucleus for subsequent authorization checking.

