# Adabas SAF Security

## An Introduction to Adabas SAF Security

Version 8.4.1

October 2022

ADABAS & NATURAL

This document applies to Adabas SAF Security Version 8.4.1 and all subsequent releases.

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



**Document ID: AAF-INTRO-841-20221009**

# Table of Contents

# 1 About this Documentation

## Document Conventions

| Convention | Description |
|---|---|
| **Bold** | Identifies elements on a screen. |
| `Monospace font` | Identifies service names and locations in the format *`folder.subfolder.service`*, APIs, Java classes, methods, properties. |
| *`Italic`* | Identifies:<br><br>Variables for which you must supply values specific to your own situation or environment.<br>New terms the first time they occur in the text.<br>References to other documentation sources. |
| `Monospace font` | Identifies:<br><br>Text you must type in.<br>Messages displayed by the system.<br>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**.

In addition, you can also access the cloud product documentation via **https://www.softwareag.cloud**. Navigate to the desired product and then, depending on your solution, go to "Developer Center", "User Center" or "Documentation".

### Product Training

You can find helpful product training material on our Learning Portal at **https://knowledge.softwareag.com**.

### Tech Community

You can collaborate with Software AG 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 AG 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 AG resources.

### Product Support

Support for Software AG 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 An Introduction to Adabas SAF Security

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:<br>■ start an Adabas nucleus<br>■ perform Adabas nucleus administration functions |
| 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:

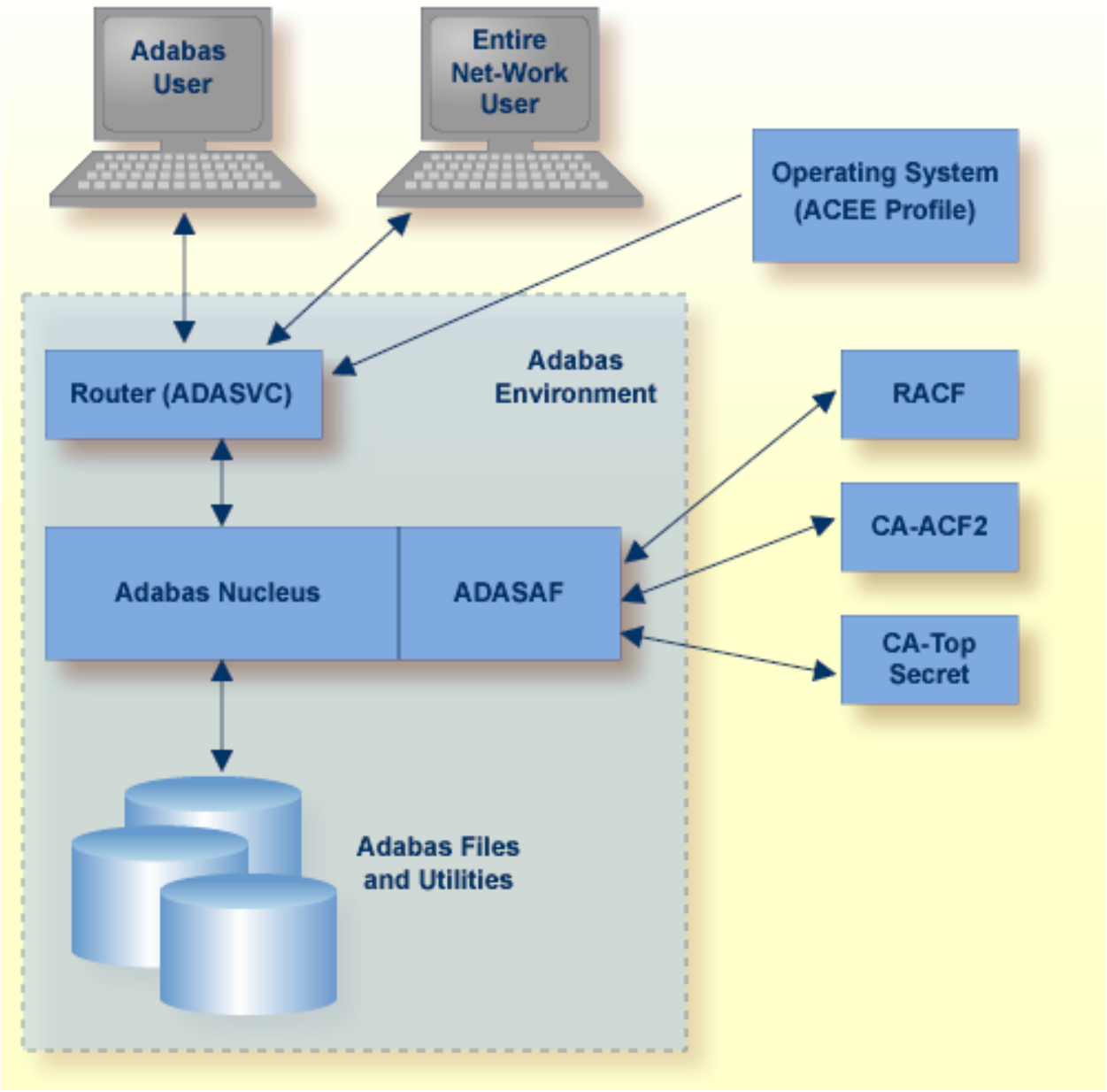
| Resource | Protection |
|---|---|
| Entire Net-work | Only authorized users are allowed to:<br>■ start an Entire Net-Work job<br>■ perform Entire Net-Work administration functions |

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.