software AG

Adabas SAF Security

Adabas SAF Security Installation

Version 8.2.2

April 2020

ADABAS & NATURAL

This document applies to Adabas SAF Security Version 8.2.2 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-INSTALL-822-20210929

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: 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 Adabas SAF Security Installation

This document describes how to install Adabas SAF Security.

Important: Before installing or upgrading, review the release notes, readmes, changes, system requirements, and installation or upgrade guide for the products you want to install. This documentation provides information you must know about the products before installing or upgrading, and also describes information you will need to provide during installation. Documentation is available on the Software AG **Empower** website.

Prerequisites

This section describes the prerequisites for Adabas SAF Security Version 8.2.

Note: For information regarding Software AG product compatibility with IBM platforms and any IBM requirements for Software AG products, please review the **Product Compatibility** for IBM Platforms web page.

Operating Systems

Adabas SAF Security is compatible with the following operating system environments:

- z/OS

Software Prerequisites

- Adabas
- Adabas Limited Library
- Adabas System Coordinator
- Natural

- Entire Net-Work

Adabas

Adabas SAF Security can be used with

- any supported level of Adabas, or
- any supported level of Adabas Cluster Services, or
- any supported level of Adabas Parallel Services.

Refer to the Adabas documentation for more information.

Note: When running an Adabas nucleus with Adabas SAF Security, Software AG recommends that you use the Adabas router and link routines for the same SM level.

Note: Adabas SAF Security requires the Adabas nucleus to run APF-authorized.

Adabas Limited Library

Adabas SAF Security uses the common SAF components supplied on the Adabas Limited Library; widely known as the WAL libraries. Adabas SAF Security Version 8.2 2 requires WAL 8.2.4 patch level 2 (WAL824P002) or above.

Adabas System Coordinator

Adabas SAF Security requires the Adabas System Coordinator. The System Coordinator libraries must be available to any Adabas nucleus or utility job that you wish to protect. You need a System Coordinator daemon if you wish to protect the online administration usage. To use online administration (SYSAAF) you must assign a System Coordinator configuration file to LFILE 152. For more information, refer to the *Adabas System Coordinator* documentation and Adabas SAF Security Installation. Adabas SAF Security does not require you to install the *Adabas System Coordinator* client component. Although it is needed for other System Coordinator based products.

Natural

Natural is required by the Online Services application SYSAAF. Any supported level of Natural can be used.

Refer to the Natural documentation for more information.

Entire Net-Work

Entire Net-Work start-up and administration functions can be protected by Adabas SAF Security.

The prerequisites for the activation of Entire Net-Work start-up protection are:

- Adabas version 8.5 SP2 or above
- Adabas SAF Security version 8.2 SP2 Patch level 2 or above

The prerequisites for providing Entire Net-Work administration function protection are:

- Entire Net-Work version 6.5 SP2 or above
- Adabas Limited Library (WAL) version 8.5 SP2 or above

Security Systems Level

Adabas SAF Security requires the following levels for the security system being used:

- CA-ACF2 Version 5 and above;
- CA-Top Secret Version 4.2 and above;
- RACF Version 2.1 and above.

Installation Data Sets (Files)

The Software AG System Maintenance Aid procedure copies the Adabas SAF Security data sets (files) from the installation medium to disk. For more specific information about the medium contents, refer to the *Software AG Product Delivery Report* that accompanies the ADASAF medium.

Installation Dataset Space Requirements

The data sets (files) are named *AAFvrs*, where *vrs* is the current Adabas SAF Security version, revision, and system maintenance level. The following are the DASD space requirements for the Adabas SAF Security installation data sets (files):

Name	3390 Disk Space Requirement
AAFvrs.LOAD	10 tracks
AAFvrs.SRCE	3 tracks
AAFvrs.JOBS	2 tracks
AAFvrs.INPL	105 tracks
AAFvrs.ERRN	2 tracks

There may also be a ZAPS data set (file) containing important last-minute corrections in AMASPZAP format and INPL update data sets (files) containing corrections to the Adabas SAF Security online system.

Installation Data Set (File) Members

AAFvrs.JOBS

The data set (file) *AAFvrs.JOBS* contains the following members:

Name	Equivalent SMA Jobs	Description
SAGI010	I020	Job to authorize ADARUN.
SAGI030	I010 and I011	This job is redundant and will be removed in the future.
SAGI050	none	This job is redundant and will be removed in the future.
SAGI055	none	Job to assemble a grouped resource name table.
SAGI060	none	Job to assemble the Adabas operator command table ADAEOPTB and link to ADAIOR.
SAGI065	none	Job to assemble grouped function mapping tables for Adabas nucleus administration functions (AAFNUCTB) and Adabas utility functions (AAFUTITB).

Installation Procedure

Before installing Adabas SAF Security, be sure that the prerequisite system configuration is available. Then perform the following steps:

- Step 13: Install the System Coordinator daemon security service

Step1: Copying the medium Contents to Disk

If you are using System Maintenance Aid (SMA), refer to the SMA documentation (included on the current edition of the Natural documentation CD). If you are not using SMA, perform steps 1a, 1b and 1c as described in this section:

- Step 1a: Copy COPY.JOB from medium to Disk
- Step 1b: Modify COPY.JOB
- Step 1c: Submit COPY.JOB

Note: If the data sets (files) for more than one product are delivered on the medium, COPY.JOB contains the JCL to unload the data sets (files) for all delivered products from the medium to your disk. After that, you will have to perform the individual install procedure for each component.

Step 1a: Copy COPY.JOB from medium to Disk

COPY.JOB (label 2) contains the JCL to unload all other existing data sets (files) from medium to disk. To unload COPY.JOB, use the following sample JCL:

```
//SAGTAPE JOB SAG,CLASS=1,MSGCLASS=X
//* --------------------------------
//COPY EXEC PGM=IEBGENER
//SYSUT1 DD DSN=COPY.JOB,
// DISP=(OLD,PASS),
// UNIT=(CASS,,DEFER),
// VOL=(,RETAIN,SER=<Tnnnnn>),
// LABEL=(2,SL)
//SYSUT2 DD DSN=<hilev>.COPY.JOB,
// DISP=(NEW,CATLG,DELETE),
// UNIT=3390,VOL=SER=<vvvvvv>,
// SPACE=(TRK,(1,1),RLSE),
// DCB=*.SYSUT1
//SYSPRINT DD SYSOUT=*
//SYSIN DD DUMMY
//
```

```
where:

<hilev>  is a valid high level qualifier
<Tnnnnn> is the tape number
<vvvvvv> is the desired volser
```

Step 1b: Modify COPY.JOB

Modify COPY.JOB to conform with your local naming conventions and set the disk space parameters before submitting this job:

- set HILEV to a valid high level qualifier
- set LOCATION to a storage location
- set EXPDT to a valid expiration date

Step 1c: Submit COPY.JOB

Submit COPY.JOB to unload all other data sets (files) from the medium to your disk.

Step 2: APF-Authorization

Ensure that the Adabas SAF Security load library and the Adabas System Coordinator load library are APF-authorized; otherwise, message AAF017 may occur and the starting job terminated.

Step 3: Link ADARUN

Execute the SAGI010 job to link ADARUN with an authorization code of 1.

Step 4: Client Considerations

Considerations relating to the various client environments are described in the following table:

Environment	Description
Batch and TSO	The external security User ID is retrieved from the ACEE address in the TCBSENV field or, if TCBSENV is not set, the User ID is retrieved from the ASXBSENV field.
Com-plete or Entire Service Manager	The external security User ID is retrieved from the ACEE address in the TCBSENV field.
CICS 4.1 or above	CICS passes the external security identifier as a parameter to the Adabas TRUE, which in turn passes the identifier on to the Adabas router. **Note:** The LGBLSET parameter `SAF=YES` must be specified in order for Adabas SAF Security to operate correctly. In addition, CICS must be configured to use an external security manager. For more information, see the Installing Adabas With TP Monitors section of the *Adabas Installation for z/OS* documentation.
IMS Version 2 and 3	The external security User ID is retrieved from the IOPCB in an IMS environment. External security must enable for the /SIGN transaction.
IMS Version 3 and above	The external security User ID is retrieved from the IOPCB or, for batch regions, from the TCB or ASXB.

Step 5: Configuration Options

You should review and make any neccessary modifications to the SAFCFG configuration options. For more information, see the section Configuration and also the *SAF Security Kernel* documentation as well as the documentation of any other Software AG SAF Security product you have installed.

The Adabas SAF Security source library contains an example member, AAFPARM, which illustrates how to set the SAFCFG configuration options relevant to running under an Adabas nucleus. You will need to create a similar source member which invokes the SAFCFG macro, specifying configuration options appropriate to how you intend to install and operate Adabas SAF Security at your site.

Step 6: Assemble and Link the SAF Modules

Using the jobs SAFI010, SAFI020 and SAFI021 supplied on the Adabas Limited (WAL) jobs library, assemble and link the site-dependent SAF Security Kernel modules: SAFCFG, SAFPSEC, and SAFPMAC.

For SAFCFG:

By default, the SAFCFG assembly job SAFI010 (supplied on the WAL jobs library) references the sample configuration source member SAFPARMS (supplied on the WAL source library). Change SAFI010 to reference your configuration module source member (see Step 5).

Also by default, SAFI010 creates a load module called SAFCFG. However, you may specify a load module name of the format A*nnnnn* to create a configuration module that will only be used by database *nnnnn*.

This is particularly useful when you have requirements that differ to the majority. For example, if database 153 has special requirements, create a configuration module called A00153 by specifying `LOADMEM=A00153` instead of `LOADMEM=SAFCFG` in a copy of job SAFI010. Adabas SAF Security will automatically use A00153 rather than SAFCFG for nucleus and utility jobs running against database 153. All other databases will continue to use SAFCFG.

For SAFPSEC:

Create the SAFPSEC security module using the sample assembly job SAFI020. Specify the appropriate STY= parameter value for your security system (RACF, TSS, or ACF2).

Note: In order to support the use of password phrases during the authentication process of Remote Workstation Logon, the SAFPSEC from WAL8.3.4 or above must be used and the REL= parameter must be set to 7730 or above. This is a pre-requisite for password phrase support in the RACROUTE macro.

FOR SAFPMAC:

Create the SAFPMAC environment module using the sample assembly job SAFI021 by referencing the configuration source member SAFPOS (supplied on the WAL source library).

For more information, see the *SAF Security Kernel* documentation in the *Administration* section of the Adabas documentation.

Optional Step for Remote Workstation Logon:

In order to improve support for the ASCII to EBCDIC translation of characters (special or otherwise) used in security credentials from remote workstations, sample job SAFI022 (supplied on the Adabas Limited (WAL) jobs library) and sample source SAFTRT (supplied on the Adabas Limited (WAL) source library) can be used to assemble a site defined translation table, SAFTRT.

If SAFTRT is available at run-time, Adabas SAF security will use it to perform ASCII to EBCDIC translation instead of its own default internal translation table.

Notes:

1. The supplied SAFTRT source is a sample translate table only, amend this translation table according to your site requirements.
2. Support for a site defined Translation Table is only available with WAL8.3.4 or above.

Step 7: Install the Operator Command Security Exit (optional)

If you wish to issue Adabas SAF Security operator commands or to use Adabas SAF Security's operator command security facility then you need to link ADAIOR with the security exit ADAEOPV (supplied on the Adabas SAF Security load library).

Additionally, the operator command grouping table ADAEOPTB (supplied on the Adabas SAF Security source library) enables you to group Adabas operator commands together into categories.

By default, job SAGI060 (supplied on the Adabas SAF Security jobs library) will assemble the operator command grouping table ADAEOPTB and link it together with ADAIOR and the ADASAF operator command security exit ADAEOPV.

If individual operator command rather than group checking is required, remove the Include statement for the module ADAEOPTB. In this case, a weak unresolved external reference for ADAEOPTB can be ignored.

Step 8: Load the Online Services Application SYSAAF

The Adabas SAF Security Online Services (SYSAAF) objects are delivered on the Adabas SAF Security distribution medium.

Use your everyday Natural INPL job to load the administration tool (Natural application SYSAAF) and associated message texts into your Natural system. For reference a sample Natural INPL job called CORI061 can be found with the sibling System Coordinator product in the *jobs* distribution file. The INPL job's work file 1 must reference the distribution file AAF*vrs*.INPL and work file 2 must reference AAF*vrs*.ERRN.

Note: If you use Natural Security in this system, define the libraries SYSAAF and SYSMX*vrs* (where *vrs* is the level you are installing, for example 821) and protect as you require. You may define MENU as the startup transaction for SYSAAF. However, you **must not** define a startup transaction for SYSMX*vrs*.

Before using SYSAAF, you must also have:

1. installed the Adabas System Coordinator configuration file (refer to the Adabas System Coordinator installation documentation) and
2. assigned the file to Natural LFILE 152, either in the Natural parameter module:

```
NTLFILE 152,dbid,file,password,cipher ↩
```

Or in your dynamic Natural parameters:

```
LFILE=(152,dbid,file,password,cipher) ↩
```

Step 9: Assemble and Link Grouped Resource Name Tables (optional)

If you wish to use grouped resource names for protecting the use of Adabas files, rather than the standard database id/file number specific names, you must define the names you wish to use and list the file numbers for which those names are to be used. You do this by assembling a set of AAFFILE macros to create a load module. The name of this load module must be provided via the FILETAB configuration option (in SAFCFG or DDSAF) and the module must be in one of the nucleus step libraries. Use the supplied sample job SAGI055 to create your grouped resource name tables.

Step 10: Check the STEPLIB Concatenation

The library containing the ADARUN module linked `AC=1` in step 3 must be first in the STEPLIB concatenation for any job start-up procedure.

Ensure that the following load libraries are APF-authorized and added to your STEPLIB concatenation:

- Adabas SAF Security load library
- The destination load library for the SAF modules created in Step 6 (if different to the Adabas SAF Security load library)
- Adabas Limited (WAL) load library
- Adabas System Coordinator load library

If you wish to protect Adabas utilities and single-user mode batch jobs, then these jobs do not have to run APF-authorized but you must ensure that the above load libraries are concatenated to the STEPLIB of these jobs.

Step 11: Security Profile and Rule Definitions

Create the necessary security profile and rule (entity) definitions required by the security package. See section Configuration for more information.

Step 12: Check the Job Control

Ensure that the job control contains an appropriate DDPRINT DD statement and, if required, DDSAF and SAFPRINT statements.

Note: DDSAF and SAFPRINT are optional. DDSAF may be used to override some SAFCFG settings for the job (see Overriding ADASAF Parameters Using DDSAF Data Set). Adabas SAF Security auto-detects DDSAF. Sample DDSAF input is supplied in the SAFPARM source library member. If DDSAF has not been specified, you will see a system message to that effect, which you can ignore. SAFPRINT contains security trace messages and is only used if the SAFCFG configuration option SAFPRINT is set to Y.

Step 13: Install the System Coordinator daemon security service

In order to protect online administration for Adabas SAF Security and sibling products Fastpath, Vista, Transaction Manager and System Coordinator you must run the security service in your System Coordinator daemon. To do this:

- Add these APF-authorized load libraries to the daemon's STEPLIB concatenation
  - The Adabas SAF Security load library.
  - The Adabas Limited (WAL) load library.
  - The load library containing your SAFCFG, SAFPMAC and SAFPSEC modules. You may use the same SAFCFG for your daemon as for your databases, or a different one and the load module may be named SAFCFG or A*nnnnn* where *nnnnn* is your daemon node-id
- Ensure the daemon job control contains an appropriate DDPRINT DD statement and, if required, SAFPRINT statements.

  

  Note: SAFPRINT DD is optional, for security trace information. It is only required when SAFCFG's SAFPRINT is set to Y (the daemon security service does not use DDSAF).

- Add a PRODUCT=AAF record to your daemon DDCARD file.