

Adabas SAF Security Installation

This document describes how to install ADASAF

- Prerequisites
 - Installation Datasets
 - Installation Procedure
-

Prerequisites

This section describes the prerequisites for Adabas SAF Security Version 8.1.2.

- Adabas
- Adabas Limited Library
- Adabas System Coordinator
- Adabas SAF Online Services
- Natural
- Security Systems Level

Adabas

Adabas SAF Security Version 8.1 and above fully support all Adabas 8.1 databases and expanded features.

Adabas Limited Library

The security kernel used by ADASAF (AAFNUC in Version 7.1 and AAFKRN in Version 7.3) has been superseded by a SAF security kernel shared by ADASAF and other Software AG SAF security products. The SAF security kernel and its associated objects were provided on the Adabas Limited Load library (WAL), starting with Version 7.4.2. There are corresponding WAL source and job libraries. Adabas SAF Security Version 8.1 requires the 8.1 Adabas Limited Library supplied with WAL 8.1.3 and above.

Objects that were formerly supplied with ADASAF and are now supplied with WAL are shown in the following table:

Old (ADASAF) Name	New (WAL) Name	Library	Function
AAFNUC (7.1) / AAFKRN (7.3)	SAFKRN	Load	SAF kernel
NA2PPRM (7.1) / AAFCFG (7.3)	SAFCFG	Source/Load	Configuration options
NA2PSEC (7.1) / AAFPSEC (7.3)	SAFPSEC	Source/Load	RACROUTE macros
NA2POS / NA2PMAC	SAFPOS / SAFPMAC	Source/Load	Operating system services
SVCLIST	SVCLIST	Load	List active Adabas SVCs
SVCSAF	SVCSAF	Load	Router security extensions
SAGI040	SAFI010	Jobs	Assemble SAFCFG
SAGI070	SAFI020	Jobs	Assemble SAFPSEC
SAGI080	SAFI021	Jobs	Assemble SAFPMAC
All source members with names beginning NA2M	Unchanged	Source	Macros used in Assemblies

Adabas System Coordinator

Adabas SAF Security Version 8.1 requires the Adabas System Coordinator Version 8.1. ADASAF needs only the database component (ADAPOP), unless you wish to use ADASAF's Online Services in a cluster environment. In this case, if you do not already know which cluster instance you want information from, you need a System Coordinator daemon to establish which instances are active. For more information, refer to the *Adabas System Coordinator* documentation and Adabas SAF Security Installation. Adabas SAF Security does not require the Adabas System Coordinator client components.

Adabas SAF Online Services

The Online Services application, SYSAAF, for Adabas SAF Security Version 8.1 is distributed in two forms:

- a demo version distributed with Adabas Version 8.1, and
- a fully operable version distributed with Adabas SAF Security Version 8.1.

In previous versions of Adabas SAF Security there was a requirement to first install the demo version prior to installing the fully operable version. This is no longer the case.

A fully operable system will be available immediately on installing the Natural INPL objects and ERRN error messages supplied on the Adabas SAF Security Version 8.1 release tape.

Note:

If you install the demo version distributed on the Adabas release tape after installing the fully operable version, then you must reapply the fully operable version from the Adabas SAF Security release tape along with any subsequently applied INPL updates.

Natural

Natural is required by the Online Services application SYSAAF.

Any supported level of Natural Version 4.1 or above can be used. Refer to the Natural documentation for more information.

Security Systems Level

ADASAF requires the following levels for the security system being used with Adabas:

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

Installation Datasets

The Software AG System Maintenance Aid procedure copies the ADASAF datasets from the installation tape to disk. For more specific information about the tape contents, refer to the *Report of Tape Creation* that accompanies the ADASAF tape.

Installation Dataset Space Requirements

The datasets are named *AAFvrs*, where *vrs* is the current ADASAF version, revision, and system maintenance level. The following are the DASD space requirements for the ADASAF installation datasets:

Dataset	3390 Disk Space Requirement
<i>AAFvrs.LOAD</i>	5 tracks
<i>AAFvrs.SRCE</i>	2 tracks
<i>AAFvrs.JOBS</i>	2 tracks
<i>AAFvrs.INPL</i>	80 tracks
<i>AAFvrs.ERRN</i>	2 tracks

There may also be a ZAPS dataset containing important last-minute corrections in AMASPZAP format and INPL update datasets containing corrections to the ADASAF online system.

Installation Dataset Members

AAFvrs.JOBS

The dataset *AAFvrs.JOBS* contains the following members:

Name	Equivalent SMA Jobs	Description
SAGI010	I020	Job to authorize ADARUN.
SAGI030	I010 and I011	Job to link the ADASAF security router (SVC). The job as distributed provides an example for temporary linking; it can be modified for permanent linking.
SAGI050	none	Job to temporarily install the ADASAF router (SVC).
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.
SAGI061	I061	Job to load ADASAF Online Services.

Installation Procedure

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

- Step1: Copying the Tape Contents to Disk
- Step 2: APF-Authorization
- Step 3: Link ADARUN
- Step 4: Relink the Adabas SVC
- Step 5: Configuration Options
- Step 6: Assemble and Link the SAF Modules
- Step 7: Install the Operator Command Security Exit (optional)
- Step 8: Load the Online Services Application SYSAAF (optional)
- Step 9: Assemble and Link Grouped Resource Name Tables (optional)
- Step 10: Check the STEPLIB Concatenation
- Step 11: Security Profile and Rule Definitions
- Step 12: Check the Job Control

Step1: Copying the Tape 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 Data Set COPY.JOB from Tape to Disk
- Step 1b: Modify COPY.JOB
- Step 1c: Submit COPY.JOB

Note:

If the datasets for more than one product are delivered on the tape, the dataset COPY.JOB contains the JCL to unload the datasets for all delivered products from the tape to your disk. After that, you will have to perform the individual install procedure for each component.

Step 1a: Copy Data Set COPY.JOB from Tape to Disk

The data set COPY.JOB (label 2) contains the JCL to unload all other existing data sets from tape 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 the 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 from the tape to your disk.

Step 2: APF-Authorization

Ensure that the Adabas load library, the ADASAF load library and the Adabas System Coordinator load library are APF-authorized; otherwise, message AAF017 occurs and the Adabas nucleus is terminated.

Step 3: Link ADARUN

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

Step 4: Relink the Adabas SVC

Before the ADASAF router can be installed, a set of router security exits must be linked. Currently, the router security extensions protect the following environments:

Environment	Description
Batch and TSO	Adabas calls from ADALNK can be secured by the external security system using ADASAF. 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	Adabas calls from ADALCO can be secured by the external security system using ADASAF. 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 ADASAF 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 <i>Adabas Installation for z/OS</i> documentation.
IMS Version 2 and 3	Adabas calls from ADALNI can be secured by the external security system using ADASAF. 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.

Note:

Job SAGI030 described below is not required when using the Adabas SVC supplied with Adabas 8.2.2 and above.

Execute SAGI030 to relink the Adabas SVC with the router security extensions supplied on the Adabas Limited Load library.

To link the security extensions with ADASVC, change the job control for either permanent or temporary installation of the SVC. Examples are provided below and in job SAGI030. For more information, see the *Adabas Installation* documentation.

Permanent Installation

For permanent installation, change the JCL as follows:

```
// EXEC PGM=IEWL
// PARM='XREF,LIST,LET,NCAL,RENT,REUS'
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSMOD DD DSN=SYS1.LPALIB,DISP=SHR (target loadlib)
//ADALIB DD DSN=user.loadlib,DISP=SHR (ADASVC loadlib)
//WALLIB DD DSN=yourdsn.LOAD,DISP=SHR (SVCSAF loadlib)
//SYSLIN DD *
MODE AMODE(31),RMODE(24)
CHANGE ADASVC(IGC00nnp) (see 'Installation Manual')
INCLUDE ADALIB(ADASVC)
INCLUDE WALLIB(SVCSAF)
NAME IGC00nnp(R)
/*
```

Temporary Installation

For temporary installation, change the JCL as follows:

```
// EXEC PGM=IEWL
// PARM='XREF,LIST,LET,NCAL,RENT,REUS'
//SYSPRINT DD SYSOUT=*
//SYSUT1 DD UNIT=SYSDA,SPACE=(CYL(1,1))
//SYSLMOD DD DSN=SYS1.LINKLIB,DISP=SHR (target loadlib)
//ADALIB DD DSN=user.loadlib,DISP=SHR (ADASVC loadlib)
//WALLIB DD DSN=yourdsn.LOAD,DISP=SHR (SVCSAF loadlib)
//SYSLIN DD *
MODE AMODE(31),RMODE(24)
INCLUDE ADALIB(ADASVC)
INCLUDE WALLIB(SVCSAF)
NAME ADASVC(R)
/*
```

Step 5: Configuration Options

You should review and make any necessary 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 ADASAF source library contains an example member, AAFPARM, which illustrates how to set the SAFCFG configuration options relevant to ADASAF. 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 ADASAF at your site.

Step 6: Assemble and Link the SAF Modules

Assemble and link the site-dependent SAF Security Kernel modules: SAFCFG, SAFSEC, and SAFPMAC, using the jobs SAFI010, SAFI020 and SAFI021 supplied on the Adabas Limited jobs library. Change the SAFCFG assembly job to reference your configuration module source member. For SAFSEC, you need to specify your security system. SAFPMAC (source SAFPOS) is assembled as supplied. For more information, see the *SAF Security Kernel* documentation.

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

To permit ADASAF to perform security validation for operator commands, modify and execute the supplied sample job SAGI060. This will assemble the command grouping table ADAEOPTB and link it together with ADAIOR and the ADASAF operator command security exit ADAEOPV.

If individual command rather than group checking is to be performed, remove the Include statement for ADAEOPTB. A weak unresolved external reference for ADAEOPTB can be ignored in this case.

Note:

ADAEOPV also enables the ADASAF operator commands.

Step 8: Load the Online Services Application SYSAAF (optional)

If you wish to use ADASAF's Online Services application SYSAAF, execute job SAGI061 to load into an appropriate Natural system file.

Note:

If Natural Security is installed, define the libraries SYSAAF and SYSMX vrs (where vrs is the version you are installing, for example 812) and protect as required. You may define MENU as the startup transaction for SYSAAF. DO NOT define a startup transaction for SYSMX vrs .

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 the Adabas start-up procedure.

Also ensure that the ADASAF load library, the target load library used in step 6 (if different), and the Adabas limited load library are APF-authorized and added to your STEPLIB concatenation.

You must also APF-authorize the Adabas System Coordinator load library and add it to your STEPLIB concatenation.

If you wish to protect Adabas utilities and single-user mode batch jobs, you must also ensure that the ADASAF, SAF Security Kernel, and Adabas System Coordinator libraries are available in the STEPLIB concatenation of those batch jobs. For utilities and single-user mode batch jobs, ADASAF does not have to run APF-authorized.

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 this nucleus (see Overriding ADASAF Parameters Using DDSAF Data Set). ADASAF 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.