Adabas SAF Security Installation

This document describes how to install ADASAF.

- Prerequisites
- Installation Data Sets (Files)
- Installation Procedure

Prerequisites

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

- Adabas
- Adabas Limited Library
- Adabas System Coordinator
- Natural
- Security Systems Level

Adabas

Adabas SAF Security Version 8.2 can be used with any supported level of Adabas Version 8.1 or above, or any supported level of Adabas Cluster Services Version 8.1 or above, or any supported level of Adabas Parallel Services Version 8.1 or above. 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 (the WAL load, jobs and source libraries). Adabas SAF Security Version 8.2 requires the Adabas Limited Libraries supplied with WAL 8.2.3 patch level 1 and above.

Adabas System Coordinator

Adabas SAF Security 8.2 requires the Adabas System Coordinator 8.2. 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 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 Data Sets (Files)

The Software AG System Maintenance Aid procedure copies the ADASAF data sets (files) 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 data sets (files) 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 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 ADASAF 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	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. This job is only required if you are using a version of the Adabas SVC below 8.2.2.
SAGI050	none	Job to temporarily install the ADASAF router (SVC). This job is only required if you are using a version of the Adabas SVC below 8.2.2.
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 (Not Required When Using the SVC from Adabas 8.2.2 and Above)
- 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
- 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
- Step 13: Install the System Coordinator daemon security service

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 COPY.JOB from Tape 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 tape, COPY.JOB contains the JCL to unload the data sets (files) 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 COPY.JOB from Tape to Disk

COPY.JOB (label 2) contains the JCL to unload all other existing data sets (files) 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 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 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 (Not Required When Using the SVC from Adabas 8.2.2 and Above)

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 *Adabas Installation for z/OS* 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 IGC00nnnp(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 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 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, SAFPSEC, and SAFPMAC, using the jobs SAFI010, SAFI020 and SAFI021 supplied on the Adabas Limited jobs library. Change the SAFCFG assembly job (SAFI010) to reference your configuration module source member. 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 some databases with different requirements 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 (job SAFI020), you need to specify your security system.

SAFPMAC (source SAFPOS) is assembled as supplied using job SAFI021.

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

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

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 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.

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 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 *nnnn* 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.