

# Installation

This section explains how to install the SAF Security Kernel. It covers the following topics:

- Prerequisites
  - Before Installing
  - Authorization
  - Modes of Operation
  - Installation Datasets
  - Installation Procedure
- 

## Prerequisites

The following are prerequisites for the SAF Security Kernel:

- OS/390 or z/os
- Adabas (or Adabas Limited Library) Version 6.2 or above
- SAF-compliant security system

## Before Installing

Before installing the SAF Security Kernel, review all possible installation options for the Kernel itself and for the product(s) it will secure. If the Kernel will execute in its own address space, allocate a unique node number to it.

## Authorization

The Kernel load library and any other step libraries in the Kernel's loading environment must be APF authorized.

## Modes of Operation

The Kernel may be embedded with a product (that is, a product that runs in the same address space). This is the case for Adabas and Entire Net-Work. To implement this mode of operation, you simply need to add the Kernel load library (and any load libraries used as the target of installation assembly and link jobs) to the step library concatenation, ensuring that they are APF authorized.

For products other than Adabas and Entire Net-Work, the Kernel operates in its own address space as a target in the Software AG network. This mode of operation is described in more detail below.

For both modes of operation, the SAF Security Kernel must run under a defined user ID. This user ID must have sufficient authority to invoke the AUTH, VERIFY, and EXTRACT functions of RACROUTE and to issue third-party checks on behalf of all users.

## Installation Datasets

The Software AG System Maintenance Aid procedure copies the SAF Security Kernel 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 tape.

### Space Requirements

**Note:**

In the following table, "vrs" stands for the version, revision, and system maintenance level.

SAKvrs.LOAD	10 tracks of 3380 disk space, 10 directory blocks
SAKvrs.SRCE	10 tracks of 3380 disk space, 10 directory blocks
SAKvrs.JOBS	5 tracks of 3380 disk space, 5 directory blocks

### Installation Dataset Overview

**Note:**

In the following table, "vrs" stands for the version, revision, and system maintenance level.

SAKvrs.LOAD	SAKvrs.LOAD is a standard load library containing modules needed to operate the SAF Security Kernel. This library must be APF-authorized and available on the loading environment of any job that includes the SAF Security Kernel.
SAKvrs.SRCE	SAKvrs.SRCE is a standard source library containing Assembler source books, macros, and examples.
SAKvrs.JOBS	SAKvrs.JOBS is a standard source library containing example jobs for installing the SAF Security Kernel.

## Installation Procedure

This section describes how to install the SAF Security Kernel. It covers the following topics:

- Assembling the Configuration Module

- 
- Assembling the RACROUTE Macros
- 
- Assembling the Operating System Services Module
- 
- Adding the Load Library
- 
- Installing the SAF Server
- 
- Configuring the SAF Server

## Assembling the Configuration Module

The configuration module defines the required installation options. Only general options are described here - product-specific options are described in the relevant product documentation. A sample job is provided in SAGI010 in the jobs library. The resulting load module, SAFCFG, must be available to the SAF Security Kernel and to the product being secured. Set these parameters to the appropriate values, as shown in the following table:

GWDBID=nnnnn	node ID of SAF server
GWSIZE=nnnnn	buffer size in K (approximately 512 bytes per user)
GWMSGL={0,1,2,3}	message level
GWSTYP={1,2,3}	security repository type

Message level indicates which diagnostic messages will be written to DDPRINT, as shown in the following table:

Message Level	Meaning
1 (default value)	Only security violations are traced.
2	Only successful checks are traced.
3	All checks are traced.
0	All tracing is suppressed.

Security type identifies the SAF security system in use, as shown in the following table:

Security Type	Meaning
1 (default value)	RACF
2	CA-Top Secret
3	CA-ACF2

## Assembling the RACROUTE Macros

The SAF Kernel requires the same version of the RACROUTE macros as used at the customer site. Sample job SAGI020 is provided to assemble the module containing these macros. Before running SAGI020, set the parameter STY to RACF, TSS, or ACF2 as appropriate and ensure that the REL parameter is set to the correct RACF version number. CA-Top Secret and CA-ACF2 require the equivalent RACF version number (for example 1.9, 2.1, or 2.2) and not the version of ACF2 or Top Secret itself. The resulting load module, SAFPSEC, must be available to the SAF Security Kernel.

## Assembling the Operating System Services Module

Sample job SAGI021 is provided to assemble the operating system services module, NA2POS. The resulting load module, SAFPMAC, must be available to the SAF Security Kernel.

## Adding the Load Library

For those products (Adabas and Entire Net-Work) that use an embedded SAF Security Kernel, you need only add the load library containing the kernel and the three load modules created above to the step library concatenation.

## Installing the SAF Server

For those products that need a SAF Security Kernel running in a separate, authorized address space, you must install a SAF Server.

The SAF server runs in its own address space, using Adabas modules to establish inter-process communication. It signs on to the Adabas SVC as a target and is therefore accessible in the same way an Adabas database is accessible. Consequently, the SAF server can be accessed remotely via Entire Net-Work.

Software AG recommends that you run the SAF server as a started task, although it may be run as a batch job. The SAF server must run APF-authorized, so all step libraries must be APF-authorized.

Additionally, the SAF server must run under a user ID with sufficient authority to invoke the RACROUTE AUTH, EXTRACT, and VERIFY functions and to make third-party checks on behalf of other users.

Sample JCL to execute the server is provided in SAGI024 in the jobs library.

## Configuring the SAF Server

The SAF server is configured by parameter input. The parameters are read from the DDCARD dataset at startup. An example dataset is provided in SAFPARMS in the source library. The following table contains a description of valid parameters, their default values, and meaning:

Parameter	Default	SVC Meaning
NODE	None	Identifies this SAF server. Must be a number between 1 and 65535 and must be unique among all targets.
PRODUCT	None	Defines which products are available on this server. Specify SAF.
FORCE	None	Defines whether or not an existing ID table entry for the same node should be overwritten. Valid values are YES and NO. Specify YES only when advised to by Software AG.
LOCAL	NO	Defines whether or not this server is to be accessible from remote users, via Entire Net-Work. Valid values are YES (the server is not accessible) and NO (the server is accessible).
NC	20	Defines the maximum number of concurrent requests that can be processed by the server. Specify a number between 1 and 32767. If a request to the server fails with response code 151, increase NC.
NABS	16	Defines the number of 4K storage blocks to be used for transmitting information between clients and the server. Specify a number between 1 and 32767. If a request to the server fails with response code 255, increase NABS.
LU	65535	Defines the maximum total length of data for a request to the server. Do not change this parameter unless advised to by Software AG.
TIMER	0	Defines how often the server is to wake up and look for work (note that the server wakes up anyway whenever it receives a request or operator command). Specify a value in seconds.
CT	60	Defines how many seconds the server will allow for a client to accept a completed request. If the client fails to acknowledge receipt of the request within this time, the server issues an ADAM93 USER GONE message and the client receives response 254. If you frequently get response 254, increase the value of CT (the maximum is 32767) and also of NC and NABS.
SVC	249	Defines which SVC number is to be used. Specify your ADABAS SVC.
MPMWTO	NO	Defines whether the server should send informational messages to the Operator console or not. You should specify YES until you are satisfied that the server is operating correctly.
DEFAULT	None	Defines the default product to which requests will be passed. Specify SAE.