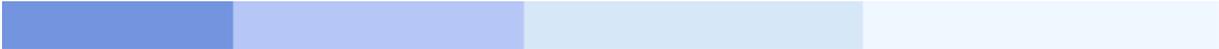




NATURAL

SAF Security Kernel

Version 1.1.1 for Mainframes



This document applies to Version 1.1.1 for Mainframes and to all subsequent releases. Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

© June 2002, Software AG
All rights reserved

Software AG and/or all Software AG products are either trademarks or registered trademarks of Software AG. Other products and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents

SAF Security Kernel	1
SAF Security Kernel	1
Introduction	2
Introduction	2
Architecture	2
Related Documentation	3
Installation	4
Installation	4
Prerequisites	4
Before Installing	4
Authorization	4
Modes of Operation	5
Installation Datasets	5
Space Requirements	5
Installation Dataset Overview	5
Installation Procedure	5
Assembling the Configuration Module	6
Assembling the RACROUTE Macros	7
Assembling the Operating System Services Module	7
Adding the Load Library	7
Installing the SAF Server	7
Configuring the SAF Server	7
Operator Commands	9
Operator Commands	9
SSHUT	9
SREST	9
SSTAT	9
SUSERS	10
SUSTAT user-id	10
SSNAP hhhhhhhh	10
SHELP	10
Security Definitions	11
Security Definitions	11
Defining Resources to RACF	11
Adding Classes to a Class Descriptor Table	11
Updating the OS/390 Router Table	12
Activating New Classes	12
Assigning a User ID for the SAF Security Started Task	12
Permitting User Access to Resource Profiles	12
Defining Resources to CA-Top Secret	12
Adding a CA-Top Secret Facility	13
Assigning a User ID for the SAF Security Started Task	13
Adding a Procedure Name for the SAF Security Started Task	13
Adding Resource Types to Resource Definition Table	13
Assigning Ownership of Resources	14
Permitting Defined Resources to Users	14
Defining Resources to CA-ACF2	14
CA-ACF2 version 5	14
CA-ACF2 version 6	15
Messages	16
Messages	16
Messages Issued by the SAF Kernel	16
Overview of Messages	16

- Operator Command Messages 20
- Overview of Messages 20
- SAF Return Codes and Started Task Messages 23**
- SAF Return Codes and Started Task Messages 23
- Return Code Structure 23
- Return Codes in SAF Trace Messages 23
- Internal Function Codes 24
- Started Task Messages 24

SAF Security Kernel

This documentation describes the SAF Security Kernel (SAK). It covers the installation, configuration, and operation of the kernel and describes the messages and codes issued by the kernel.

This documentation is intended for system administrators or others who are responsible for installing the SAF Security Kernel or administering and maintaining the SAF Security Kernel as part of a SAF security solution.

The SAF Security Kernel documentation is organized as follows:

	Introduction
	Installation
	Operator Commands
	Security Definitions
	Messages
	Codes and Started Task Messages

Introduction

The System Authorization Facility (SAF) is used by OS/390 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.

Architecture

A SAF security solution comprises two separate components:

- a product-specific component that is distributed and installed with the product being protected (Adabas, Natural, Entire Net-Work, or EntireX)
- a product-independent SAF kernel (the subject of this document) which may either be embedded in an authorized product or operate as a separate authorized server

The SAF Security Kernel acts as an agent for other Software AG products such as Adabas, Natural, and Entire Net-Work, allowing them to secure resources via a SAF-compliant security system, thus enhancing the scope of the security system to enable:

- a single control and audit system for all resources
- a single definition of user IDs and passwords
- industry standard protection of resources such as Adabas data and Natural libraries
- maximized return on investment in the security repository

Related Documentation

For details about securing specific products, please refer to the relevant product documentation:

- Adabas SAF Security
- Natural SAF Security
- Entire Net-Work
- EntireX Security

Some of the above products are distributed with their own copy of the SAF kernel. The individual product documentation indicates if this is the case or if the product uses the independent SAF kernel.

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)
GWMSGSL={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.

Operator Commands

MVS operator communication with the SAF Server is achieved using the OS/390 Modify (F) command. All operator commands for the SAF Kernel are prefixed with SAF. For example:

```
F jobname ,SAF SSTAT
```

The available operator commands are:

- SSHUT
 - SREST
 - SSTAT
 - SUSERS
 - SUSTAT user-id
 - SSNAP hhhhhhhh
 - SHELP
-

SSHUT

Perform an orderly shutdown of the SAF Kernel started task. This command should always be used to request an orderly termination.

SREST

Restart the SAF Kernel, ensuring that all data held in its cache is flushed. Any data held by the security system itself in the SAF Kernel address space is also flushed. The operation is transparent to all on-line and batch users.

SSTAT

Display general statistics on the operator console for the SAF Kernel.

SUSERS

Display a list of active users.

SUSTAT user-id

Display statistics for a specified user.

SSNAP hhhhhhh

Display a selected portion of the SAF Kernel's memory. Operation is not terminated.

SHELP

Display all possible SAF Kernel operator commands.

Security Definitions

SAF Security is implemented by defining resource classes and profiles and permitting users the necessary access to those profiles. Specific requirements for class and profile definitions and access levels are described in the individual product documentation. This section describes in general how to define resources to RACF, CA-Top Secret and CA-ACF2. It covers the following topics:

- Defining Resources to RACF
 - Defining Resources to CA-Top Secret
 - Defining Resources to CA-ACF2
-

Defining Resources to RACF

This section describes how the resources are defined to RACF. It covers the following topics:

- Adding Classes to a Class Descriptor Table
- Updating the OS/390 Router Table
- Activating New Classes
- Assigning a User ID for the SAF Security Started Task
- Permitting User Access to Resource Profiles

For detailed procedures, refer to the IBM manual for the installed version of RACF.

Adding Classes to a Class Descriptor Table

1.
Add the resource classes to the RACF Class descriptor table. Refer to the IBM SPL RACF manual. For an example, see IBM SYS1.SAMPLIB, member RACINSTL.
2.
For flexibility, allocate maximum length for the classes (80).
- 3.

Define the classes to enable discrete and generic profile use.

4.

Check further attributes controlling the level of RACF messages generated when performing RACROUTE calls, as well as the required level of SMF recording. Sample definitions are provided in source member RACFCLSX.

Updating the OS/390 Router Table

Update the OS/390 router table as described in the IBM SPL RACF manual. For an example, see the IBM SYS1.SAMPLIB, member RACINSTL, section RFTABLE.

Activating New Classes

Activate new resource classes with SETROPTS (refer to the *IBM RACF Command Language Reference* manual). For an example, activate class NBKSAG:

```
SETROPTS CLASSACT(NBKSAG)
SETROPTS GENCMD(NBKSAG)
SETROPTS GENERIC(NBKSAG)
```

Assigning a User ID for the SAF Security Started Task

The SAF Security Kernel runs either in its own Started Task or in an Adabas or Entire Net-Work started task. Assign a user ID to these jobs with the relevant RACF authorizations, including the ability to perform RACROUTE, TYPE=EXTRACT, TYPE=AUTH and TYPE=VERIFY calls on profiles belonging to the defined classes

Permitting User Access to Resource Profiles

After adding profiles to protect the different resources, permit users the required level of access, using the relevant RACF Commands. The following example adds resource profile "etb.policy.quote1" and grants READ access to user ID "user2" and CONTROL access to "user3". "user2" represents a client and requires READ access to execute while "user3" represents a server component that requires CONTROL access in order to register:

```
RDEFINE NBKSAG ETB.POLICY.QUOTE1 UACC(NONE)
PERMIT ETB.POLICY.QUOTE1 CLASS(NBKSAG) ACCESS(READ) ID(USER2)
PERMIT ETB.POLICY.QUOTE1 CLASS(NBKSAG) ACCESS(CONTROL) ID(USER3)
```

Defining Resources to CA-Top Secret

This section describes how resources are defined to CA-Top Secret. It covers the following topics:

- Adding a CA-Top Secret Facility
- Assigning a User ID for the SAF Security Started Task
- Adding a Procedure Name for the SAF Security Started Task

-
- Adding Resource Types to Resource Definition Table
-
- Assigning Ownership of Resources
-
- Permitting Defined Resources to Users

For detailed procedures, refer to the Computer Associates manual for the installed version of CA-Top Secret.

Adding a CA-Top Secret Facility

CA-Top Secret enables a set of authorization checks to be made against a certain facility. For example, this can be used to secure the development environment SAGDEV separately from the production environment SAGPROD. Alternatively, a default facility of batch can be used.

When adding additional facilities, use the following attributes:

```
AUTHINIT , MULTIUSER , NONPWR , PGM=ADA , NOABEND
```

Assigning a User ID for the SAF Security Started Task

Add one user ID for each instance of the SAF Security Started Task. If required, different facilities can be assigned to development and production tasks.

The designated facility is assigned to the Started Task user ID, as follows:

```
TSS CRE(user-id) DEPT(dept) MASTFAC(fac)
```

Adding a Procedure Name for the SAF Security Started Task

The procedure name under which the SAF Security Started Task executes must be defined to CA-Top Secret, as follows:

```
TSS ADD(STC) PROC(proc) USER(user-id)
```

Different procedure names are suggested when securing different environments separately with the use of non-default CA-Top Secret facilities.

Adding Resource Types to Resource Definition Table

Add the resource types to the CA-Top Secret Resource Definition Table (RDT). Below is an example for resource type NBKSAG. Refer to the CA-Top Secret Reference Guide for a detailed explanation of the following commands and arguments:

```
TSS ADD(RDT) RESCLASS(NBKSAG)
RESCODE(HEXCODE)
ATTR(LONG)
ACLST(NONE, READ, CONTROL)
DEFACC(NONE)
```

Assigning Ownership of Resources

Assign ownership to a particular resource as shown in the following example. This must be done before permitting access to defined resource profiles:

```
TSS ADD(user1) NBKSAG(etb.policy.quote1)
```

This makes user "user1" the owner of the Broker service "etb.policy.quote1".

Permitting Defined Resources to Users

Permit access to a resource profile as shown in the following example.

```
TSS PER(user2) NBKSAG(etb.policy.quote1) FAC(fac) ACCESS (READ)
```

This permits user "user2" READ access to the Broker service "etb.policy.quote1". This enables the user to execute as a client and issue requests to this Broker service:

Defining Resources to CA-ACF2

This section describes the definition of resources to CA-ACF2 versions 5 and 6. For detailed procedures, refer to the Computer Associates manual for the installed version of CA-ACF2.

Note:

CA-ACF2 provides insufficient return codes to determine whether a resource profile does not exist or is simply not accessible to the user. Therefore, if access is denied by CA-ACF2, the SAF Security Kernel will always report "Access denied resource not allowed" in the error message. Consequently, the SAF Security configuration options such as BKUNI=Y to allow access to undefined resources are not applicable where CA-ACF2 is used.

CA-ACF2 version 5

1.

The SAF Security Kernel executes as a normal started task in OS/390. Define the user ID of the task to CA-ACF2 with the following attributes:

```
MUSASS, NON-CNCL, STC
```

To avoid the NON-CNCL attribute, APAR TW95626 must be applied.

2.

Activate the SAF Interface using the following command:

```
GSO OPTS - SAF
```

3.

Switch off all SAF checks by inserting the SAFSAVE record as follows:

```
SAFSAVE CLASSES(-) CNTLPTS(-) SUBSYS(-)
```

4.

Switch on the SAF security checks for the SAF Security Kernel by inserting the SAFPROT record as follows:

```
CLASSES(-) CNTLPTS(-) SUBSYS(ADARUN)
```

5.

For the general resource class names used by SAF Security product options, define a 3-character CA-ACF2 resource type code by inserting a SAFMAPS record as follows:

```
SAFMAPS MAPS(NBK/NBKSAG)
```

6.

Define the required resource profiles to CA-ACF2 using the new type code. The following example shows the addition of a Broker service "etb.policy.quote1", allowing READ access for user ID "user2":

```
$KEY(etb.policy.quote1) TYPE(NBK) UID(user2) ALLOW SERVICE(READ)
```

CA-ACF2 version 6

1.

The SAF Security Kernel executes as a normal started task in OS/390. Define the user ID of the server task to CA-ACF2 with the following attributes:

```
MUSASS,STC
```

Note:

CA-ACF2 version 6.1 and 6.2 no longer require TW95626, as these versions are more SAF-compliant.

2.

Insert the SAFDEF records as follows:

```
SAFDEF.EXS1
FUNCRET(4) FUNCRSN(0) ID(ENTIREX) MODE(GLOBAL)
RACROUTE(REQUEST=VERIFY SUBSYS=ADARUN REQSTOR=-)
RETCODE(4)
SAFDEF.EXS2
FUNCRET(4) FUNCRSN(0) ID(ENTIREX) MODE(GLOBAL)
RACROUTE(REQUEST=AUTH SUBSYS=ADARUN REQSTOR=-)
RETCODE(4)
SAFDEF.EXS3
FUNCRET(4) FUNCRSN(0) ID(ENTIREX) MODE(GLOBAL)
RACROUTE(REQUEST=EXTRACT SUBSYS=ADARUN REQSTOR=-)
RETCODE(4)
```

3.

For the general resource class names used by SAF Security product options, define a 3-character CA-ACF2 resource type code by inserting a CLASMAP record as follows

```
CLASMAP
ENTITYLN(0) MUSID() RESOURCE(NBKSAG) RSRCTYPE(NBK)
```

4.

Define the required security profiles to CA-ACF2 using the new type code. The following example shows the addition of a Broker service "etb.policy.quote1", allowing READ access only for user ID "user2":

```
$KEY(ETB) TYPE(NBK)
policy.quote1 UID(user2) SERVICE(READ) ALLOW
policy.quote1 UID(-) PREVENT
```

Messages

This section contains the following:

- Messages Issued by the SAF Kernel
- Operator Command Messages

Messages Issued by the SAF Kernel

The following messages are displayed on the operator console and system message datasets. The messages are issued by the SAF Kernel component and other products into which SAF Security is installed such as Natural, Entire Broker, Entire Net-Work, and Adabas SQL Server.

Overview of Messages

SEFM001 | SEFM002 | SEFM004 | SEFM006 | SEFM008 | SEFM009 | SEFM013 | SEFM014 | SEFM015 | SEFM016 | SEFM017 | SEFM020 | SEFM021 | SEFM025 | SEFM026 | SEFM028 | SEFM029 | SEFM030 | SEFM031 | SEFM040 | SEFM041 | SEFM042 | SEFM043 | SEFM049 | SEFM050 | SEFM255

SEFM001 *SSSSSSSS : user : resource

Explanation The security system determined that the identified user does not have authorization for the identified resource. System return and reason codes are given in the hexadecimal string SSSSSSSS. This message is displayed when access has been denied to a particular resource.

SEFM002 *XX to request FF : user : resource

Explanation An unexpected response code XX was received from the SAF Kernel for the identified user when requesting function FF to be performed.

SEFM004 *NATURAL programs not extracted

Explanation The SAF Kernel was not able to extract a list of protected program objects from the security system on behalf of Natural users.

User Action Obtain a trace of "SAF call: RACROUTE EXTRACT" from the security system and contact Software AG technical support. ACF2 and Top Secret users should ensure that the protected programs have been extracted from the security system and supplied to the SAF Kernel via the SEFEXT DD statement in the started task JCL.

SEFM006 *ADARSP XX(xx) to request FF : user

Explanation The SAF Kernel returned Adabas response XX and subresponse xx to request FF for user.

User Action Ensure that the SAF Kernel started task is active. Check its output for error messages. Take the necessary remedial action indicated by the Adabas response code.

SEFM008 *SAF Security Kernel (Vx.x) started

Explanation The SAF Kernel start-up completed.

User Action Informational message only.

SEFM009 *Module MMMMMMMM not loaded

Explanation The SAF Kernel could not load the identified module.

User Action Ensure that the module is in the steplib and the region size is sufficient.

SEFM013 *Less storage acquired than specified

Explanation The SAF Kernel was not able to GETMAIN all the storage required to satisfy the buffer size specified in its parameters.

System Action Operation continues.

User Action Ensure region size is sufficient and parameters are appropriate.

SEFM014 *No storage could be acquired

Explanation The SAF Kernel could not obtain any storage at system start-up.

System Action Operation has terminated.

User Action Ensure region size is sufficient and system parameters are appropriate.

SEFM015 *Logic error - XXXX for request FF : user

Explanation The SAF Kernel suffered an internal error.

System Action A general restart is performed and operation continues.

User Action Keep all information written to DDPRINT and contact your Software AG technical support representative.

SEFM016 *SAF logoff failed SSSSSSSS ACEE AAAA : user

Explanation The SAF Kernel was unable to logoff the identified user from the security system. The SAF error code is SSSSSSSS.

User Action Contact your Software AG technical support representative.

SEFM017 *Insufficient space to initialize - make NATURAL buffer XX

Explanation The Natural SAF interface requires a larger value to be specified for the length of the IDMSBUF parameter.

User Action Increase the value assigned to the Natural IDSIZE parameter.

SEFM020 *GETMAIN failed / IDSIZE error

Explanation The Natural SAF interface could not acquire storage from the designated IDMSBUF.

User Action Increase Natural region and/or thread size.

SEFM021 *Illegal storage use / relocation problem

Explanation Internal problem in Natural SAF storage use.

User Action Contact your Software AG technical support representative.

SEFM025 *NATURAL IDMSBUF parameter not defined

Explanation The Natural IDSIZE parameter has not been specified.

User Action Ensure IDSIZE is set correctly in the Natural parameters.

SEFM026 *NATURAL protected programs not extracted code: XX

Explanation The list of protected programs could not be returned from the SAF Kernel to Natural.

User Action Ensure the same copy of the configuration module SAFCFG is used by all system components. Check that the GWSTYP parameter defined in SAGI010 and STY parameter in SAGI020 are both correctly set for the installed security system and that all installation requirements have been met.

SEFM028 *System files not found in environment table

Explanation The current Natural system files were not matched in the table defining all possible system file sets.

User Action Ensure that the environment definitions in Natural Security are correct.

SEFM029 *Error in communications layer - check installation procedure

Explanation Possible reasons for error: Adabas link module installed into this component is not reentrant.

SEFM030 *SQL table / view could not be identified for file (XX,YY)

Explanation The interface component could not identify the table name for DBID/FNR of an SQL request.

User Action Ensure that the interface is correctly installed, and contact your Software AG technical support representative.

SEFM031 *DBID / FNR identified with SQL request not recognized XXXX

Explanation The interface component could not determine the DBID/FNR associated with this SQL request.

User Action Contact your Software AG technical support representative.

SEFM040 *Interface installed for S/390 NATURAL

Explanation The interface is installed for operation with S/390 Natural.

User Action Informational message only.

SEFM041 *Interface installed for NET-WORK

Explanation The interface is installed for operation with Entire Net-Work.

User Action Informational message only.

SEFM042 *Interface installed for BROKER

Explanation The interface is installed for operation with Entire Broker.

User Action Informational message only.

SEFM043 *Interface installed for ADABAS SQL SERVER

Explanation The interface is installed for operation with Adabas SQL Server.

User Action Informational message only.

SEFM049 *User type T not permitted by installed options

Explanation The SAF Kernel will not permit the identified user type to operate using the currently installed options.

SEFM050 *Error writing SMF record : XX

Explanation The identified error occurred when writing an SMF record.

SEFM255 *Unauthorized use of request

Explanation An illegal use of security request was attempted.

User Action Contact your Software AG technical support representative.

Operator Command Messages

The following messages are displayed in response to operator commands being processed by the SAF Kernel.

Overview of Messages

SEFM900 | SEFM901 | SEFM909 | SEFM910 | SEFM911 | SEFM913 | SEFM914 | SEFM918 | SEFM919

SEFM900 *Operator issued command: XXXXXXXXX

Explanation SAF Security Kernel received the stated operator command.

User Action Informational message only.

SEFM901 *SAF SECURITY KERNEL - general statistics (at hhhhhhhh)

Explanation The operator issued the command to display general statistics. The address in the first line is the address of the SAF Kernel's storage cache.

General Statistics	SEFM901 * SAF SECURITY KERNEL - SERVER STATISTICS (AT 12C47000)						
	SEFM902 * RESOURCE	CHECK(+VE)	CHECK(-VE)	CHECK	SAVED	OVERWRITES	LEN
	SEFM903 * APPLICATION	10	0	0	0	0	8
	SEFM903 * DBMS CHECK	0	0	0	0	0	17
	SEFM903 * SYSMAIN	0	0	0	0	0	21
	SEFM903 * SYSTEM FILE	2	0	0	0	0	40
	SEFM903 * PROGRAM	0	0	0	0	0	17
	SEFM903 * BROKER	0	0	0	0	0	68
	SEFM903 * NET-WORK	0	0	0	0	0	17
	SEFM903 * SQL SERVER	0	0	0	0	0	32
	SEFM903 * USERS - ACTIVE:	1	FREE: 2051	OVERWRITES:	0		

SEFM909 *SAF Security Kernel - shutdown initiated

Explanation The operator issued the command to shut down the SAF Kernel started task.

SEFM910

Explanation The operator issued the command to display statistics for all currently active users.

Active Users Statistics	SEFM910 * SAF SECURITY KERNEL - LIST ALL ACTIVE USERS						
	SEFM911 * USERID	CHECK(+VE)	CHECK(-VE)	CHECK	SAVED	OVERWRITES	BUFF
	SEFM912 * K11079	3	0	0	0	0	0

SEFM911 *userid xxxxxxxx

Explanation The operator issued the command to display statistics for a specific currently active user.

Userid xxxxxxxx Statistics	SEFM911 * SJU	CHECK(+VE)	CHECK(-VE)	CHECK	SAVED	OVERWRITES	BUFF
	SEFM912 * APPLICATION	10	0	0	0	0	10
	SEFM912 * DBMS CHECK	0	0	0	0	0	0
	SEFM912 * SYSMAIN	0	0	0	0	0	0
	SEFM912 * SYSTEM FILE	2	0	0	0	0	2
	SEFM912 * PROGRAM	0	0	0	0	0	0
	SEFM912 * BROKER	0	0	0	0	0	0
	SEFM912 * NET-WORK	0	0	0	0	0	0
	SEFM912 * SQL SERVER	0	0	0	0	0	0

SEFM913 *No active users found in SAF SECURITY KERNEL

Explanation No active users were found in the SAF Security Kernel.

SEFM914 *Requested user xxxxxxxx

Explanation The requested user was not found in the SAF Security Kernel.

SEFM918 *SUPPLIED ADDRESS IS OUTSIDE OF LEGAL RANGE

Explanation An attempt was made to snap storage outside the bounds of the SAF Kernel's cache.

SEFM919 *OPERATOR COMMAND DID NOT CONTAIN REQUIRED ARGUMENT(S)

Explanation A required parameter was omitted from an operator command. For example, SUSTAT with no userid specified.

SAF Return Codes and Started Task Messages

The SAF Kernel displays an eight-byte code containing various return and reason codes from SAF. This information is shown in a number of messages denoted "SSSSSSSS".

This section covers the following topics:

- Return Code Structure
 - Return Codes in SAF Trace Messages
 - Internal Function Codes
 - Started Task Messages
-

Return Code Structure

The SAF return codes have the following structure:

Position within Message Code	Information Content
Byte 1	SAF Return Code (R15 after RACROUTE)
Byte 2	Internal Function Code
Byte 3	RACROUTE Return Code
Byte 4	RACROUTE Reason Code
Bytes 5 - 8	Internal Reason Code

Return Codes in SAF Trace Messages

The SAF trace messages written to DDPRINT, when GWMSGSL is not 0, include the first four bytes of the return code (as shown in the table above) printed as eight hexadecimal digits:

Position within Trace Message	Information Content
Digits 1 and 2	SAF Return Code (R15 after RACROUTE)
Digits 3 and 4	Internal Function Code
Digits 5 and 6	RACROUTE Return Code
Digits 7 and 8	RACROUTE Reason Code

Refer to the IBM manual *External Security Interface (RACROUTE) Macro Reference* manual for MVS and VM for a thorough explanation of all possible return/reason codes. CA-Top Secret and CA-ACF2 can provide different return code values in some circumstances.

Internal Function Codes

SAF Kernel internal function codes include the following:

Function Code (Hex)	Description
00	Authorize Natural Library
04	Authorize Adabas Access
08	Authorize SYSMAIN Function
0C	Authorize Natural System Files
10	Authorize Natural Program Execution
14	Authorize Broker Service
18	Authorize Entire Net-Work Access
1C	Authorize SQL Server Access
44 or 6C	Authenticate User

Started Task Messages

These messages are issued when the SAF Security Kernel is executing in its own started task. They simply echo the values of the DDCARD parameters:

SPMMP004 INPUT PARAMETER: NODE=10005
SPMMP004 INPUT PARAMETER: SVC=249
SPMMP004 INPUT PARAMETER: PRODUCTS=SAF
SPMMP004 INPUT PARAMETER: LOCAL=NO
SPMMP004 INPUT PARAMETER: NABS=50
SPMMP004 INPUT PARAMETER: NU=100
SPMMP004 INPUT PARAMETER: NC=50
SPMMP004 INPUT PARAMETER: TIMER=600
SPMMP004 INPUT PARAMETER: LU=32768
SPMMP004 INPUT PARAMETER: CT=120
SPMMP004 INPUT PARAMETER: FORCE=NO

The following confirms that the SAF Security node is active:

SPMMP011 TARGET 10005 IS ACTIVE

The following confirms that an operator command has been received and processed:

SPMMP012 OPER TYPEIN: SAF operator-command
SPMMP021 OPERATOR COMMAND PROCESSED SUCCESSFULLY

The following confirms that the started task has terminated normally:

SPMMP014 TARGET 10005 TERMINATION IN PROGRESS
ADAM97 10005 THIS ASCB/INITIATOR WILL BE TERMINATED BY MVS AT EOJ
SPMMP015 TARGET 10005 ENDED NORMALLY