

SEFM* - ADASAF SAF Interface and SAF Security Kernel Messages

ADASAF displays an eight-byte code containing various return codes from SAF. This information is shown in a number of messages denoted *sssssss*.

The ADASAF return code "sssssss" contains the following structure:

Position	Information Content
Byte: 1	SAF return code
Byte: 2	Function code. ADASAF internal function codes (hex) include: 04 Authorize Adabas access 44 or 6C Authenticate user
Byte: 3	Return code from security system, for example RACF
Byte: 4	Reason code from security system, for example RACF
Bytes: 5 - 8	SAF reason code

Refer to the IBM manual External Security Interface (RACROUTE) Macro Reference manual for z/OS and z/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.

The following message groups are described:

- Messages Displayed on the Operator Console and System Message Data Sets (SEFM001 - SEFM255)
- Operator Command Messages (SEFM900+ Series)

Messages Displayed on the Operator Console and System Message Data Sets (SEFM001 - SEFM255)

The following messages are displayed on the operator console and system message datasets. The messages may be issued by the SAF Security Kernel component (in a daemon, an Adabas nucleus or an Entire Net-Work node) or by another product into which SAF Security is installed, such as Natural or Entire Broker.

Overview of Messages

BLS0334	SEFM001	SEFM002	SEFM004	SEFM006	SEFM008	SEFM009
SEFM013	SEFM014	SEFM015	SEFM016	SEFM017	SEFM020	SEFM021
SEFM025	SEFM026	SEFM028	SEFM029	SEFM030	SEFM031	SEFM041
SEFM049	SEFM050	SEFM051	SEFM205	SEFM210	SEFM255	

BLS0334 SYMBOL 'NETSAF' CANNOT BE FOUND. LOADING ABORTED

Explanation This message should be ignored.

SEFM001 ssssssss : user : resource

Explanation The security system determined that the user identified in the message (*user*) does not have authorization for the resource listed in the message (*resource*). System return and reason codes are given in the hexadecimal string *sssssss*. 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 Security Kernel for the user identified in the message (*user*) when requesting function *FF* to be performed on the resource specified in the message (*resource*).

SEFM004 *Natural programs not extracted

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

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

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

Explanation The SAF Security Kernel returned the Adabas response code (*XX*) and subcode (*xx*) shown in the message to request *FF* for the user shown in the message (*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 Gateway (Vv.r) started
*** SAF Security Kernel (Vx.x.x - BUILD xxxx) started**

Explanation Entire Net-Work SAF Security Interface (ADASAF) startup completed or the SAF Security Kernel initialized successfully.

Action No action is required for this informational message.

SEFM009 Module *module-name* not loaded

Explanation Entire Net-Work SAF Security Interface could not load the module listed in the message (*module-name*).

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

SEFM013 *Less {memory | storage} acquired than specified

Explanation The SAF Security Kernel or the Entire Net-Work SAF Security Interface (ADASAF) were not able to allocate all the memory or storage required to satisfy the buffer size specified in its parameters. Operation continues.

Action Ensure that the region size is sufficient and the parameters are appropriate.

SEFM014 *No {memory | storage} could be acquired

Explanation Entire Net-Work SAF Security Kernel or the SAF Security Interface (ADASAF) could obtain no storage or memory at system startup. Operation has terminated.

Operation has terminated.

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

SEFM015 *Logic error - XXXX for request FF : *user*

Explanation The SAF Security Kernel suffered an internal error. A general restart is performed and the operation continues.

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 Security Kernel was unable to logoff *user* from the security system. The SAF error code is ssssssss.

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 NSF`SIZE`.

Action Increase the Natural NSF`SIZE` parameter.

SEFM020 *GETMAIN failed / IDSIZE error

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

Action Increase Natural region and/or thread size.

SEFM021 *Illegal storage use / relocation problem

Explanation Internal problem in Natural SAF storage use.

Action Contact your Software AG technical support representative.

SEFM025 *Natural IDMSBUF parameter is not defined

Explanation The Natural NSF`SIZE` parameter has not been specified.

Action Ensure NSF`SIZE` 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 Security Kernel to Natural.

Action Ensure the same copy of the configuration module SAFCFG is used by all system components. Check that the GWSTYP parameter defined in SAFI010 and STY parameter in SAFI020 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.

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 / VIEview could not be identified for file (XX,YY)

Explanation Interface could not identify table name for DBID/FNR of an SQL request.

Action Ensure interface is correctly installed, then contact your Software AG technical support representative.

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

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

Action Contact your Software AG technical support representative.

SEFM041 *Interface installed for Net-work

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

Action No action is required for this informational message.

SEFM049 *User type T not permitted by installed options

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

SEFM050 *Error writing SMF record : XX

Explanation The stated error occurred when an SMF record was being written.

SEFM051 *SAFPRINT dataset not defined, DDPRINT will be used

Explanation SAFPRINT=Y is set in SAFCFG, but no SAFPRINT dataset is defined.

SEFM205 *CPU identity : *cpuid*

Explanation The interface component linked to Entire Net-Work displays the CPU ID of the host machine.

Action No action is required for this informational message.

SEFM210 ***SAF Gateway is active for Entire Net-Work**

Explanation The Entire Net-Work SAF Security Interface is active.

Action No action is required for this informational message.

SEFM255 ***Unauthorized use of request**

Explanation Attempted illegal use of security request.

Action Contact your Software AG technical support representative.

Operator Command Messages (SEFM900+ Series)

The following messages are displayed in response to operator commands:

Overview of Messages

SEFM900 | SEFM901 | SEFM902 - 905 | SEFM909 | SEFM910 | SEFM911 |
 SEFM913 | SEFM914 | SEFM915 | SEFM916 | SEFM918 | SEFM919 | SEFM920 |
 SEFM921 | SEFM922 | SEFM923 | SEFM924 | SEFM928 | SEFM929

SEFM900 *** Operator issued command: *command***

Explanation Entire Net-Work SAF Security Interface (ADASAF) or the SAF Security Kernel received the operator command identified in the message.

Action No action is required for this informational message.

SEFM901 * SAF server - General statistics (at *hhhhhhhh*)
 * SAF Security Kernel - General statistics (at *hhhhhhhh*)

Explanation The operator command for general statistics was issued. Here is an example of the statistics messages produced for the SAF server:

SEFM901	* SAF SERVER - GENERAL STATISTICS (AT <i>hhhhhhhh</i>)					
SEFM902	* RESOURCE	CHECK(+VE)	CHECH(-VE)	CHECK SAVED	OVERWRITES	LEN
SEFM903	* APPLICATION	1	0	0	0	8
SEFM903	* ADABAS	0	0	0	0	32
SEFM903	* SYSMAIN	0	0	0	0	13
SEFM903	* SYSTEM FILE	2	0	0	0	24
SEFM903	* PROGRAM	0	0	0	0	17
SEFM903	* BROKER	0	0	0	0	32
SEFM903	* NET-WORK	0	0	0	0	0
SEFM903	* SQL SERVER	0	0	0	0	0
SEFM904	* USERS - ACTIVE: 1 FREE: 55 OVEWRITES: 0					

Here is an example of the statistics messages produced for the SAF Security Kernel:.
 The address in the first line is the address of the SAF Kernel's storage cache.

SEFM901	* SAF SECURITY KERNEL - SERVER STATISTICS (AT 12C47000)					
SEFM902	* RESOURCE	CHECK(+VE)	CHECH(-VE)	CHECK SAVED	OVERWRITES	LEN
SEFM903	* APPLICATION	10	0	0	0	8
SEFM903	* DBMS CHECK	0	0	0	0	17
SEFM903	* SYSMAIN	0	0	0	0	21
SEFM903	* SYSTEM FILE	2	0	0	0	40
SEFM903	* PROGRAM	0	0	0	0	17
SEFM903	* BROKER	0	0	0	0	68
SEFM903	* NET-WORK	0	0	0	0	17
SEFM903	* SQL SERVER	0	0	0	0	32
SEFM904	* CACHED USERS:	1	HIGH WATERMARK:	1	MAX USERS:	5545
SEFM905	* OVERWRITES:	0	AUTHENTICATED:	0	DENIED:	0

Action No action is required for this informational message.

SEFM902 - 905 *statistics*

Explanation Various statistics for the SAF server and the SAF Security Kernel are displayed. See message SEFM901.

Action No action is required for this informational message.

SEFM909 * {SAF Gateway | SAF Security Kernel} - shutdown initiated

Explanation The operator issued a command to shut down Entire Net-Work SAF Security Interface or the daemon started task (SAF Security Kernel). This message is also issued when a secure Adabas nucleus, Net-Work node or Adabas SQL server terminates.

Action No action is required for this informational message.

SEFM910 *{SAF Server | SAF Security Kernel} - list all active users

Explanation The operator issued a command to display a list of currently active users.

The following is a sample of the output produced for the SAF server:

SEFM910	*	SAF SERVER	-	LIST ALL ACTIVE USERS					
SEFM911	*	USERID		CHECK(+VE)	CHECH(-VE)	CHECK	SAVED	OVERWRITES	BUFF
SEFM912	*	K11079		3	0		0	0	0

The following is a sample of the output produced for the SAF Security Kernel:

```
SEFM910 * SAF GATEWAY - LIST ALL ACTIVE USERS
SEFM911 * USERID CHECK(+VE) CHECH(-VE) CHECK SAVED OVERWRITES BUFF
SEFM912 * K11079          3          0          0          0          0
```

Action No action is required for this informational message.

SEFM911 *userid...

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

The following is a sample of the output produced for the SAF server:

SEFM911	*	NXB		CHECK(+VE)	CHECH(-VE)	CHECK	SAVED	OVERWRITES	BUFF
SEFM912	*	APPLICATION		1	0		0	0	0
SEFM912	*	DBMS CHECK		0	0		0	0	0
SEFM912	*	SYSMAIN		0	0		0	0	0
SEFM912	*	SYSTEM FILE		2	0		0	0	0
SEFM912	*	PROGRAM		0	0		0	0	0
SEFM912	*	BROKER		0	0		0	0	0
SEFM912	*	NET-WORK		0	0		0	0	0
SEFM912	*	SQL SERVER		0	0		0	0	0

The following is a sample of the output produced for the SAF Security Kernel:

```
SEFM911 * SJU          CHECK(+VE) CHECH(-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
```

Action No action is required for this informational message.

SEFM913 * **No active users found in SAF {Server | Gateway | Security Kernel}**

Explanation No active users were found in Entire Net-Work SAF Security Interface (ADASAF) or in the SAF Security Kernel.

Action No action is required for this informational message.

SEFM914 * **Requested user *userid* not found in SAF {Server | Gateway | Security Kernel}**

Explanation The requested user was not found in the Entire Net-Work SAF Security Interface (ADASAF) or in the SAF Security Kernel.

Action No action is required for this informational message.

SEFM915 **SEFM915 * SAF Security Kernel - snap of server memory**

Explanation This message is issued in response to an SSNAP operator command and is followed by a sequence of SEFM916 messages.

Action No action is required for this informational message.

SEFM916 * ***hhhhhhhh hhhhhhhh hhhhhhhh hhhhhhhh hhhhhhhh.x..X.Y/***

Explanation This message contains the results of an SSNAP command. Each SSNAP snaps up to 256 bytes and shows the address, the hexadecimal storage contents, and the interpretation.

Action No action is required for this informational message.

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 arguments**

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

Action Correct the operator command and try again.

SEFM920 **SSNAP, SSTAT, SUSERS, SUSTAT, SREST, SNEWCOPY, SLOGOFF, STRACE**

Explanation This message is issued in response to an SHELP operator command and lists the valid SAF Kernel operator commands.

Action No action is required for this informational message.

SEFM921 * **Memory allocation failure - users cannot be logged off**

Explanation The SAF Kernel was unable to obtain temporary storage (approximately 16Kb) to log users off in response to an SREST , SNEWCOPY or SLOGOFF operator command.

Action Increase the region size.

SEFM922 * **User *userid* logged off**

Explanation This message is issued in response to an SLOGOFF operator command. The indicated user has been logged off from the security system.

Action No action is required for this informational message.

SEFM923 * **User *userid* not logged off - user not found**

Explanation This message is issued in response to an SLOGOFF operator command. The requested user could not be found in the SAF Kernel's cache.

Action Verify the correct user ID was specified.

SEFM924 * **User *userid* not logged off - return code ZZ**

Explanation This message is issued in response to an SLOGOFF operator command. An internal error (indicated by ZZ) occurred while attempting to log the requested user off.

Action Evaluate the return code to determine the cause of the error.

SEFM928 * **Invalid trace setting - must be 0, 1, 2 or 3**

Explanation The STRACE operator command was issued with an invalid trace setting.

Action Correct the trace setting and try again.

SEFM929	* Invalid SAF Security Kernel operator command
Explanation	An invalid SAF Security Kernel operator command was entered.
Action	Specify a valid SAF Security Kernel operator command.