Adabas SAF Security

Adabas SAF Security Messages and Codes

Version 8.1.3

June 2008

Adabas SAF Security

This document applies to Adabas SAF Security Version 8.1.3 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.

Table of Contents

1 Adabas SAF Security Messages and Codes

ADASAF Messages

AAF001 Unable to load required modules

A required module could not be loaded. Operation terminates with an abend U0042.

Check that all required modules are available.

AAF002 Unable to allocate required storage

There is insufficient memory available for ADASAF to operate. Operation terminates with an abend U0042.

Increase the amount of memory (above the 16-megabyte line) available to the failing job.

AAF003 dbid Unable to allocate NRS storage

ADASAF needs approximately 2KB of memory below the 16-megabyte line. If the memory is not available at initialization (or after a `newcopy` operator command), ADASAF issues this message and operation terminates.

Ensure that enough memory is available.

AAF004 dbid Module xxxxxxxx not loaded

The indicated module could not be loaded during initialization or during the `newcopy` operator command. If the module is required (rather than optional), operation terminates.

Ensure that the module is available.

AAF005 dbid Invalid parameters detected

One or more invalid parameters were specified in DDSAF. Operation terminates.

Correct the invalid parameters.

AAF006 dbid Allocation of user file cache failed

ADASAF allocates a user file cache above the 16-megabyte line. If the storage is not available at initialization (or after a `newcopy` operator command), ADASAF issues this message and operation terminates.

Ensure that enough storage is available or reduce the `MAXFILES` parameter (this may adversely affect performance).

AAF007 dbid INPUT PARAMETER

ADASAF echoes the parameters read from DDSAF for information and auditing purposes.

None.

AAF008 dbid Invalid parameter: INPUT PARAMETER

ADASAF detected incorrect input in DDSAF. AAF008 is issued for each invalid parameter found and is followed by message AAF005.

Correct the invalid parameter.

AAF009 dbid Allocation of Password/Cipher Code cache failed

There is insufficient storage available above the 16-megabyte line to allocate the table. Each entry requires 16 bytes and the table has a 32-byte header. Operation terminates.

Ensure that enough storage is available.

AAF010 dbid Password/Cipher Code cache too small - increase MAXPC

ADASAF found more passwords and/or cipher codes in RACF than it could store in its table. Operation terminates.

Increase the `MAXPCC` parameter.

AAF011 dbid Error extracting Passwords/Cipher Codes from RACF

ADASAF could not extract passwords and cipher codes from RACF. Operation terminates.

Check that you have specified the correct resource class and entity name format. Activate tracing and check for any errors or warnings. Check the system log for RACF messages.

AAF012 dbid Adabas SAF VX.X.X is active in XXXX mode

ADASAF has successfully initialized in FAIL or WARN mode, as indicated by XXXX.

None.

AAF015 dbid Newcopy of Configuration module failed

After a `newcopy` operator command, ADASAF was unable to reload SAFCFG. Operation terminates.

This error occurs only if there is a shortage of storage or the module SAFCFG was deleted from the load library after initialization. Determine which of these is the case and correct it.

AAF016 dbid Newcopy reinitialization failed

This message appears after a failure during `newcopy` processing. It should be accompanied by a more detailed error message specifying the nature of the failure.

Take the action recommended by the accompanying message.

AAF017 dbid Not APF authorized

ADASAF must run APF-authorized. Operation terminates.

Check that all STEPLIBs are in the APF list and that ADARUN is linked with `AC(1)`.

AAF018 dbid No security details for job JOBNAME

This message appears when an unsecured Adabas call is received from the indicated job.

The most likely cause is an installation error, either of the Adabas Router security extensions or of the Adabas link module.

AAF019 dbid ADASAF initialization error(s) - Nucleus will terminate

This message appears after an initialization error and is preceded by a more specific error message.

Take the action recommended by the accompanying message.

AAF020 dbid Unable to add ADASAF Smart Management PIN

This message appears during initialization if ADASAF fails to activate its Adabas Error Handling interface.

None. ADASAF continues, with its Error Handling interface disabled.

AAF021 dbid NOTOKEN is set - calls from unsecured clients are allowed

The configuration option `NOTOKEN` has been activated. No security checks will be performed for unsecured mainframe clients. See the configuration parameter `NOTOKEN`.

None.

AAF022 dbid Incompatible Configuration module detected

ADASAF has detected an incompatible Configuration module. The nucleus session terminates.

Ensure that the Configuration module is created using the macros supplied with the version of ADASAF you wish to use.

AAF023 dbid Invalid xxxx parameter returned by ADASAFX2

Your password/cipher code exit has returned incorrect data, as indicated by xxxx:

- type: the returned code type was neither password nor cipher code
- code: no password/cipher code was returned
- file: no file number was returned

The nucleus session terminates.

Correct your exit.

AAF024 ADASAF installation error: SAFPMAC not linked REUSable

ADASAF cannot initialize because the module SAFPMAC has not been linked with the `REUS` attribute. The nucleus session terminates.

Ensure that SAFPMAC is linked `REUS,NORENT`.

AAF028 dbid SAF Kernel initialization error - Nucleus will terminate

The SAF Kernel could not initialize for some reason (indicated by a SEFMxxx message preceding the AAF028 message). The Adabas nucleus terminates.

Correct the problem which prevents the SAF Kernel from initializing (for example, increase region size or modify SAFCFG options) and restart the Adabas nucleus.

AAF029 dbid No access to class/resource

The execution security check made when starting a nucleus or utility has failed. The job abends U0042. *Class* and *resource* show the resource class and profile name against which the check was made.

Check that the security class and resource name are correct and that they have been defined to the external security system, with the appropriate access permissions.

ADAEOPV Messages

The following messages in response to operator commands may be issued by ADAEOPV, if you have linked it with ADAIOR.

AAF101 SAF VIOLATION

The operator command is not permitted for this Adabas nucleus.

Review operator command security definitions for this Adabas nucleus.

AAF102 NO ADAEOPTB

ADAEOPTB (operator command grouping table) is in use but does not contain an entry for this operator command.

Ensure the operator command was entered correctly. Review the contents of ADAEOPTB and add this command if necessary.

AAF103 AAF NOT FOUND

ADAEOPV could not locate the Adabas SAF Security load module.

Review the Adabas SAF Security installation and ensure that it is active in this Adabas nucleus.

SAF Security Kernel Messages

SAF Security Kernel messages are described in the *SAF Security Kernel* documentation.

Adabas Response Codes

The following Adabas response codes can result from ADASAF processing:

Code	Meaning
200	The command could not satisfy the necessary security checks. This response code may be accompanied by one of the following subcodes: ■ 0: standard user check failed ■ 1: no free user file cache entry for workstation user ■ 2: cross-level security check failed ■ 3: no security information available for command ■ 4: timeout during workstation logon ■ 5: internal SAF Kernel error ■ 6: failure during newcopy/restart operation. The nucleus terminates.
207	Internal ADASAF and ADALNK two-phase response code for remote workstation logon. This code is normally not displayed or presented.

Code	Meaning
208	ADASAF response code indicating that two-phase logon can continue. If this internal response code is displayed or otherwise presented, the wrong ADALNK version for workstation logon is being used.
209	Workstation user's password has expired. This code is normally not returned to the application. Instead the workstation user is prompted to enter a new password.

SAF Return Codes

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

Return Code Structure

The ADASAF return code contains the following structure:

Position Within Message Code	Information Content
Byte: 1	SAF return code (R15 after RACROUTE)
Byte: 2	Function code (see below)
Byte: 3	RACROUTE return code
Byte: 4	RACROUTE reason code
Bytes: 5 - 8	Internal reason code

The ADASAF trace messages include the first four bytes of this information, 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	Function code (see below)
Digits 5 and 6	RACROUTE return code
Digits 7 and 8	RACROUTE reason code

Refer to the *IBM Security Server RACROUTE Macro Reference* manual 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

ADASAF internal function codes include:

Function Code (Hex)	Description
04	Authorize Adabas access
18	Authorize cross-level access
44 or 6C	Authenticate user

Diagnosis of Violations

If security violation logging is active, the SAF Security Kernel includes additional diagnostic information about the violation in its trace message. This information is described in the *SAF Security Kernel* documentation.