Adabas SAF Security

Adabas SAF Security Configuration Parameters

Version 8.3.1

October 2021

ADABAS & NATURAL

This document applies to Adabas SAF Security Version 8.3.1 and all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: AAF-PARAMETERS-831-20210928

Table of Contents

1 About this Documentation

Document Conventions

Convention	Description
Bold	Identifies elements on a screen.
`Monospace font`	Identifies service names and locations in the format *`folder.subfolder.service`*, APIs, Java classes, methods, properties.
`Italic`	Identifies: Variables for which you must supply values specific to your own situation or environment. New terms the first time they occur in the text. References to other documentation sources.
`Monospace font`	Identifies: Text you must type in. Messages displayed by the system. Program code.
{ }	Indicates a set of choices from which you must choose one. Type only the information inside the curly braces. Do not type the { } symbols.
|	Separates two mutually exclusive choices in a syntax line. Type one of these choices. Do not type the | symbol.
[ ]	Indicates one or more options. Type only the information inside the square brackets. Do not type the [ ] symbols.
...	Indicates that you can type multiple options of the same type. Type only the information. Do not type the ellipsis (...).

Online Information and Support

Software AG Documentation Website

You can find documentation on the Software AG Documentation website at **https://documentation.softwareag.com**.

Software AG Empower Product Support Website

If you do not yet have an account for Empower, send an email to empower@softwareag.com with your name, company, and company email address and request an account.

Once you have an account, you can open Support Incidents online via the eService section of Empower at **https://empower.softwareag.com/**.

You can find product information on the Software AG Empower Product Support website at **https://empower.softwareag.com**.

To submit feature/enhancement requests, get information about product availability, and download products, go to **Products**.

To get information about fixes and to read early warnings, technical papers, and knowledge base articles, go to the **Knowledge Center**.

If you have any questions, you can find a local or toll-free number for your country in our Global Support Contact Directory at **https://empower.softwareag.com/public_directory.aspx** and give us a call.

Software AG Tech Community

You can find documentation and other technical information on the Software AG Tech Community website at **https://techcommunity.softwareag.com**. You can:

- Access product documentation, if you have Tech Community credentials. If you do not, you will need to register and specify "Documentation" as an area of interest.
- Access articles, code samples, demos, and tutorials.
- Use the online discussion forums, moderated by Software AG professionals, to ask questions, discuss best practices, and learn how other customers are using Software AG technology.
- Link to external websites that discuss open standards and web technology.

Data Protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR). Where applicable, appropriate steps are documented in the respective administration documentation.

2 Adabas SAF Security Configuration Parameters

This document describes the Adabas SAF Security configuration parameters.

Caution: Because of the sensitivity of SAF security, the ability to change the configuration module or the DDSAF dataset must be tightly controlled by the external security system.

Parameters Specified in Configuration Module SAFCFG

This section describes the site-dependent parameters which are used by Adabas SAF Security. These parameters are specified using an assembled configuration module SAFCFG. SAFCFG is supplied as part of the SAF Security Kernel on the Adabas limited (WAL) libraries.

Note: The default value for each Adabas SAF Security parameter is underlined in the parameter syntax definition.

AAFPRFX: Use Resource Name Prefix

Parameter	Description	Syntax
AAFPRFX	Enter a 1 to 8 character prefix which will be used as the first element of any resource profile names checked by Adabas SAF Security. For example, specifying AAFPRFX=TEST,DBFLEN=1,DELIM=Y will cause accesses to database 153, file 12 to be checked against a resource profile named TEST.CMD00153.FIL00012. The default is no prefix. **Note:** The prefix specified in SAFCFG may be overridden by DDSAF input. However, because DDSAF is not used for utilities, the nucleus and utility start checks are performed using the prefix defined in SAFCFG.	AAFPRFX=xxxxxxxx

ABS: Adabas Basic Services Level Protection

Parameter	Description	Syntax
ABS	Level of protection for Adabas Basic Services: ■ 0: disables ADASAF protection for Adabas Basic Services ■ 1: ADASAF is to protect main functions only ■ 2: ADASAF is to protect both main and subfunctions See also the section Adabas Basic Services.	ABS={0| 1 | 2 }

ADASCR: Use Logon ID of Security Package as Adabas Security Password

Parameter	Description	Syntax
ADASCR	Indicates whether or not the Logon ID of the security package is to be used as the Adabas Security password. ■ N: the Logon ID of the security package is not to be used as the Adabas Security password ■ Y: the Logon ID is placed in the Additions 3 field of the Adabas control block for use by Adabas ■ G: the caller's SAF group is placed in the Additions 3 field of the Adabas control block for use by Adabas.	ADASCR={N | Y | G }

ALLFILES: Clients Have Same Permissions for All Files in a Database

Parameter	Description	Syntax
ALLFILES	Indicates whether or not client sessions have the same permissions for all files in a database: ■ N: Client session security checks are performed for each file accessed and updated. File-related cache data and statistical information is maintained. ■ Y: Client session security checks are performed only once at first file access and first file update. If the client session's first file access/update is permitted, then all subsequent access/updates to other files are also permitted without the need to perform further security checks. No file-related cache data or statistical information is maintained. Do not specify ALLFILES=Y for databases where clients have different permissions for different files. **Note:** The use of this parameter requires Adabas Limited Library (WAL) version 8.5 SP3 or above.	ALLFILES={N | Y }

CIPHER: Extract Adabas Cipher Codes from RACF

Parameter	Description	Syntax
CIPHER	Indicates whether or not ADASAF should extract Adabas cipher codes from RACF and apply them to the relevant Adabas commands. ■ N: ADASAF should not extract Adabas cipher codes from RACF and apply them to the relevant Adabas commands ■ Y: ADASAF will extract Adabas cipher codes from RACF and apply them to the relevant Adabas commands	CIPHER={N| Y }

DBADMIN: Database Administration Protection

Parameter	Description	Syntax
DBADMIN	Indicates whether or not to protect nucleus administration functions: ■ N: Nucleus administration functions are not protected ■ Y: Nucleus administration functions are protected For DBADMIN=Y only: ■ NOFILE: File-level protection is not enabled ■ FILE: File-level protection is enabled And: ■ WARN: A failed security check will not result in RSP200 ■ FAIL: A failed security check will result in a RSP200 A setting of WARN may be useful during the DBADMIN=Y implementation phase, to identify the required security definitions without impacting the execution of administration requests. See also the section Nucleus Administration Functions.	DBADMIN={N|(Y, ↩ NOFILE|FILE, ↩ WARN|FAIL)}

DBAUDIT: Database Audit Logging for Adabas Security Violations

Parameter	Description	Syntax
DBAUDIT	Indicates whether or not to perform nucleus audit logging for Adabas Security violations: ■ N: No auditing will be performed ■ Y: Auditing will be performed See also the section Nucleus Audit Logging for Adabas Security Violations.	DBAUDIT={N|Y}

DBCLASS: Database Resource Class Name

Parameter	Description	Syntax
DBCLASS	The name of the resource class name for use in authorization checks performed by Adabas SAF Security for: ■ *Operation in the Adabas Nucleus* ■ *Operation in Adabas Utilities* ■ *Operation in the Adabas System Coordinator Daemon* ■ *Operation in Entire Net-Work*	DBCLASS={ name ↩ | ↩ (name,FASTAUTH) ↩ }

Parameter	Description	Syntax
	The name can be up to eight alphanumeric characters and the supplied default is DBCLASS=ADASEC. Notes on the use of FASTAUTH: 1. The FASTAUTH option for DBCLASS only affects Adabas SAF Security operation in Adabas nuclei and Entire Net-Work nodes. 2. The FASTAUTH option results in the building of in-storage profiles (shared globally in a data space) for the resources of the specified class name. 3. Whenever any profile is updated, the security administrator must issue a SETROPTS RACLIST(*classname*) REFRESH to cause the globally shared in-storage profiles to be refreshed. This process of refreshing by SETROPTS must be completed **before** issuing AAF SREST operator commands to all relevant jobs operating with Adabas SAF Security in order to discard any locally cached security information. 4. The FASTAUTH option reduces the number of security-related zIIP switches for Adabas nuclei and Entire Net-Work nodes running with ADARUN ZIIP=YES. 5. The FASTAUTH option can be turned on or off dynamically by re-assembling SAFCFG accordingly and issuing the AAF SNEWCOPY operator command to all relevant jobs operating with Adabas SAF Security. 6. The FASTAUTH option requires Adabas Limited Library (WAL) version 8.5 SP3 or above.	

DBFLEN: Format of Database ID and File Number in Resource Profiles

Parameter	Description	Syntax
DBFLEN	The format of the Database ID and file number in resource profiles: ■ 0: 3 digits with leading zeroes ■ 1: 5 digits with leading zeroes ■ 2: up to 5 digits with leading zeroes suppressed The default value is recommended to simplify reporting and maintenance of security profiles; to allow for the large Database IDs and file numbers introduced with Adabas version 6; and to allow for ET data protection, if required.	DBFLEN={ 0 ↩ |1| 2 }

DBNCU: Number of Database Checks to be Buffered Per User

Parameter	Description	Syntax
DBNCU	The number of database checks to be buffered per user, in the cache defined by GWSIZE. These buffered checks are used to avoid repeated SAF calls for a user when LOGOFF=NEVER or LOGOFF=TIMEOUT is specified.	DBNCU=0

DBUNI: Allow Access to Undefined Adabas Resources

Parameter	Description	Syntax
DBUNI	Indicates whether or not access to undefined Adabas resources should be allowed. The normal mode of operation is to prevent access to resources not defined to the security system. Profiles representing Adabas resources are added to the security repository with either a default access or by granting access to specific users and groups. ■ N: access to undefined Adabas resources is not allowed ■ Y: access to undefined Adabas resources is allowed **Note:** This option does not permit access to resources defined with universal access "none". **Note:** DBUNI is ignored when checking whether a nucleus or utility is allowed to execute.	DBUNI={N| Y ↩ }

DELIM: Delimiter Usage for Entity Names

Parameter	Description	Syntax
DELIM	Use of delimiter when defining an entity name. ■ N: the entity name begins with ACC for access commands and UPD for update commands and does not contain a full stop (period) delimiter ■ Y: the entity name begins with CMD and has a full stop (period) delimiter between the Database ID and file number	DELIM={ N | Y}

ETDATA: Protect Commands Which Access or Create ET Data

Parameter	Description	Syntax
ETDATA	Indicates whether or not ADASAF should protect commands that access or create ET data. ■ N: ADASAF should not protect commands that access or create ET data ■ Y: ADASAF should protect commands that access or create ET data This parameter is only honored if fixed-length Database IDs and file numbers are used in the resource profile names (that is, the DBFLEN parameter specifies 0 or 1). File number 00000 (DBFLEN=1) or 000 (DBFLEN=0) is checked for the relevant database. RE commands need read access; OP commands with Command Option 2 set to E need read access; ET, CL, and C3 commands with Command Option 2 set to E need update access.	ETDATA={ N | Y }

FAILUTI: Fail mode for Adabas utility jobs

Parameter	Description	Syntax
FAILUTI	Indicates the action to be taken when an Adabas utility SAF security check fails. ■ YES: the utility job abends U0042. This is the default. ■ NO: the security violation is ignored and the utility job is allowed to continue. A setting of NO may be useful during the Adabas SAF Security implementation phase, to identify the required security definitions without impacting the execution of utility jobs.	FAILUTI={YES | NO}

FILETAB: Name of Load Module Containing Grouped Resource Names

Parameter	Description	Syntax
FILETAB	The name of the load module containing grouped resource names for this nucleus. Grouped resource names can be used instead of database/file number when checking access to an Adabas file. The load module is created using the AAFFILE macro (see *Defining Grouped Resource Names with AAFFILE* and its name must be a valid load module name of up to 8 characters. The default is not to use grouped resource names.	FILETAB=xxxxxxxx

GROUP: Use Group ID for Resource Authorization Checking

Parameter	Description	Syntax
GROUP	Indicates whether or not the Group ID rather than the User ID is to be used for resource authorization checking. ■ N: Group ID is not to be used for resource authorization checking ■ Y: Group ID is to be used for resource authorization checking	GROUP={ N | Y }

GWMSGL: Trace Level for Security Checking

Parameter	Description	Syntax
GWMSGL	The tracing level for security checks. ■ 0: no tracing ■ 1: trace violations only ■ 2: trace successful checks only ■ 3: trace all checks Use the parameter SAFPRINT to control where the trace messages are written and, for an interpretation of the trace message content, refer to section *Interpreting Trace Messages* in the SAF Security Kernel documentation. These traces messages will be retained for as long as the job, or the dataset to which they have been written, remains available. Deleting the job, or dataset, will delete the trace messages. For diagnostic and troubleshooting purposes, the content of the trace message includes the SAF User ID for which access was requested.	GWMSGL={ 0 | 1 ↩ | 2 | 3 } ↩

GWSIZE: Storage Size for Caching User Information

Parameter	Description	Syntax
GWSIZE	The amount of storage (in kilobytes) to be used for caching user information related to the security system, for example checked entity names. For optimum performance in conjunction with LOGOFF=NEVER|TIMEOUT, ensure that GWSIZE is large enough to allow effective caching. For more information, see the description of LOGOFF and the topic *Caching of Security Checks* in section *Operation in the Adabas Nucleus*.	WAL 812: GWSIZE=16 ↩ WAL 813 and above: GWSIZE=256

GWSTYP: Adabas SAF Security Type

Parameter	Description	Syntax
GWSTYP	The SAF security type. ■ 1: RACF ■ 2: CA-Top Secret ■ 3: CA-ACF2 ■ 4: RACF executing on a Fujitsu operating system.	GWSTYP={ 1 | 2 | 3 | 4 }

HOLDCMD: Access Requirement For Commands Which Place Records On Hold

Parameter	Description	Syntax
HOLDCMD	Determines whether hold commands (L4, L5, L6, S4 and HI) require READ access (the default) or UPDATE access. You may decide to require UPDATE access to prevent inadvertent holding of records by clients who only have READ access impacting clients who have genuine UPDATE access.	HOLDCMD={ R | U }

LFPROT: Protect LF (Read FDT) Command

Parameter	Description	Syntax
LFPROT	Specify whether or not the LF command is protected. ■ Y: the SAF User ID which issued the LF command must have read access to the relevant file ■ N: no security check is performed for LF commands	LFPROT={ Y | N}

LOGOFF: Logging Off ADASAF Users

Parameter	Description	Syntax
LOGOFF	Indicates when ADASAF should log off users from the SAF security system. ■ ALWAYS: ADASAF is to log off the user whenever the associated Adabas user session ends, either because of a Close command or because the Adabas user has been stopped or timed out. ■ NEVER: ADASAF is to log off the user only when the user's memory (in the cache specified by GWSIZE) needs to be allocated to a new user. ■ TIMEOUT: ADASAF is to log off the user only when the associated Adabas user session has been timed out or stopped.	WAL 812: LOGOFF={ ALWAYS ↩ | NEVER | ↩ TIMEOUT } WAL 813 and above: LOGOFF={ ALWAYS ↩ | NEVER ↩ | TIMEOUT }

Parameter	Description	Syntax
	The settings LOGOFF=NEVER and LOGOFF=TIMEOUT will substantially reduce SAF overheads in databases where users often issue Close commands and then start a new session. However, it may be necessary to increase GWSIZE to provide enough memory to save the user details across Close commands. Use the Adabas session statistics "Number of users participating" and "Number of commands executed" to decide whether LOGOFF=NEVER or LOGOFF=TIMEOUT should be used. If the number of commands per user is relatively low, consider setting LOGOFF=TIMEOUT and then using ADASAF's Online Services to monitor the effectiveness of GWSIZE: option 1 shows the number of allocations (new users created) and overwrites (old users deleted); if these are high, increase GWSIZE. If the Adabas non-activity timeout values are such that users are frequently timed out, set LOGOFF=NEVER rather than LOGOFF=TIMEOUT.	

MAXFILES: Maximum Number of Files to be Cached Per User

Parameter	Description	Syntax
MAXFILES	The number of files for which security information is to be cached for each user. If a user accesses more than this number of files, the oldest entries will be overwritten.	MAXFILES={ nnnn | 16 }

MAXPCC: Maximum Number of Passwords and Cipher Codes

Parameter	Description	Syntax
MAXPCC	The maximum number of passwords and cipher codes to be extracted from RACF for the current Adabas nucleus. If ADASAF finds more than this number, nucleus initialization is terminated with message AAF010.	MAXPCC={ nnnn | 16}

NETADMIN: Entire Net-Work Administration Protection

Parameter	Description	Syntax
NETADMIN	Indicates whether or not to protect Entire Net-Work administration functions: ■ N: Entire Net-Work administration functions are not protected ■ Y: Entire Net-work administration functions are protected For NETADMIN=Y only: ■ WARN: A failed security check will not result in RSP200	NETADMIN={N|(Y, ↩ WARN|FAIL)}

Parameter	Description	Syntax
	■ FAIL: A failed security check will result in a RSP200 A setting of WARN may be useful during the NETADMIN=Y implementation phase, to identify the required security definitions without impacting the execution of administration requests. See also the section *Entire Net-Work Administration Functions*.	

NOTOKEN: Allow Calls from Unsecured Mainframe Clients

Parameter	Description	Syntax
	Indicates whether or not calls from unsecured mainframe clients are to be allowed. An unsecured mainframe client is a client operating in an environment that does not provide security information via the Adabas router. For example, a remote Lpar where the router has not been linked with the SAF security extensions (SVCSAF) or a CICS job that is using an Adabas link globals module that specifies `SAF=NO`. ■ N: Calls from unsecured mainframe clients are not to be allowed ■ Y: Calls from unsecured mainframe clients are to be allowed **Caution:** It is strongly recommended not to use `NOTOKEN=Y` since this may allow unauthorized access to or updating of Adabas data. `NOTOKEN=Y` is only intended for extremely short-term use during a phased implementation of Adabas SAF Security.	`NOTOKEN={ N ↩ | Y }`

NWCLASS: Class Name for Cross-Level Checking

Parameter	Description	Syntax
`NWCLASS`	The name of the resource class name for use in cross-level authorization checks performed by Adabas SAF Security for *Operation in the Adabas Nucleus*. The name can be up to eight alphanumeric characters and the supplied default is `NWCLASS=ADASEC`. Notes on the use of `FASTAUTH`: 1. The `FASTAUTH` option for `NWCLASS` only affects Adabas SAF Security operation in Adabas nuclei. 2. The `FASTAUTH` option results in the building of in-storage profiles (shared globally in a data space) for the resources of the specified class name. 3. Whenever any profile is updated, the security administrator must issue a SETROPTS RACLIST(*classname*) REFRESH to cause the globally shared in-storage profiles to be refreshed. This process of refreshing by	`NWCLASS={ name ↩ | ↩ (name,FASTAUTH) ↩ }`

Parameter	Description	Syntax
	SETROPTS must be completed **before** issuing `AAF SREST` operator commands to all relevant jobs operating with Adabas SAF Security in order to discard any locally cached security information. 4. The `FASTAUTH` option reduces the number of security-related zIIP switches for Adabas nuclei running with ADARUN ZIIP=YES. 5. The `FASTAUTH` option can be turned on or off dynamically by re-assembling SAFCFG accordingly and issuing the `AAF SNEWCOPY` operator command to all relevant jobs operating with Adabas SAF Security. 6. The `FASTAUTH` option requires Adabas Limited Library (WAL) version 8.5 SP3 or above.	

NWNCU: Number of Database Checks to be Buffered per Cross-Level User

Parameter	Description	Syntax
`NWNCU`	The number of database checks to be buffered per cross-level user, in the cache defined by `GWSIZE`.	`NWNCU=0`

NWUNI: Allow Access to Undefined Adabas Resources for Cross-Level Checking

Parameter	Description	Syntax
`NWUNI`	Indicates whether or not access to undefined Adabas resources should be allowed for cross-level checks. The normal mode of operation is to prevent access to resources not defined to the security system. Profiles representing Adabas resources are added to the security repository with either a default access or by granting access to specific users and groups. ■ N: access to undefined Adabas resources is not allowed for cross-level checks ■ Y: access to undefined Adabas resources is allowed for cross-level checks **Note:** This option does not permit access to resources defined with universal access "none".	`NWUNI={ N ↩ | Y }`

NWUSRW: User ID for Security Checking for Workstation Users

Parameter	Description	Syntax
NWUSRW	The User ID to be used for database cross-level security checks issued on behalf of workstation users.	NWUSRW=WINUSER

PASSWORD: Extract Adabas Passwords from RACF

Parameter	Description	Syntax
PASSWORD	Indicates whether or not ADASAF should extract Adabas passwords from RACF and apply them to the relevant Adabas commands. ■ N: ADASAF should not extract Adabas passwords from RACF and apply them to the relevant Adabas commands ■ Y: ADASAF should extract Adabas passwords from RACF and apply them to the relevant Adabas commands	PASSWORD={N | Y ↩ }

PCPROT: Protect PC (Invoke Stored Procedure) Command

Parameter	Description	Syntax
PCPROT	Specify whether or not the PC command is protected. ■ N: no security checking of the PC command ■ R: the SAF User ID which issued the PC command must have READ access to the file specified in the PC command ■ U: the SAF User ID which issued the PC command must have UPDATE access to the file specified in the PC command **Note:** This configuration option has no influence on checking of commands issued by stored procedures. Those commands are always checked for the appropriate security access to the appropriate resource.	PCPROT={ N ↩ | R | U}

REMOTE: Mechanism for Protecting Calls from Remote Users

Parameter	Description	Syntax
REMOTE	The mechanism ADASAF should use to protect calls from remote users. ■ LINK: ADASAF is to use, as the SAF Logon ID, the Entire Net-Work link name by which the call arrived ■ NODE: ADASAF is to use, as the SAF Logon ID, the Entire Net-Work node name from which the call arrived	REMOTE={ LINK | ↩ NODE | NONE ↩ | POPUP}

Parameter	Description	Syntax
	■ NONE: this setting must only be used in conjunction with Entire Net-Work SAF Security ■ POPUP: ADASAF is to initiate the remote workstation logon procedure	

SAFPRINT: Security Check Trace Message Printing

Parameter	Description	Syntax
SAFPRINT	Specify whether security check trace messages should be written to DD SAFPRINT or to DD DDPRINT. ■ N: security check trace messages are to be written to DD DDPRINT ■ Y: security check trace messages are to be written to DD SAFPRINT If SAFPRINT=Y is specified, but a SAFPRINT dataset is not provided, the trace messages will be written to DDPRINT. The SAFPRINT dataset must be defined in the nucleus JCL and may refer to a SYSOUT dataset or to a file defined with RECFM=F (or FB) and LRECL=121.	SAFPRINT={N ↩ | Y }

UTI: Utility Protection Level

Parameter	Description	Syntax
UTI	Indicates the level of protection for Adabas Utilities: ■ 1: Name-level protection (default level) ■ 2: Function-level protection ■ 3: Function/File-level protection See also the section Utility Start-up.	UTI={1|2|3}

WTOCASE: Mixed or Upper Level Case for ADASAF Prefix Messages

Parameter	Description	Syntax
WTOCASE	The AAF prefix messages issued by ADASAF may be written in mixed or upper case. For compatibility with previous versions, the default is upper case. ■ M: AAF prefix messages are to be written in mixed case ■ U: AAF prefix messages are to be written in upper case	WTOCASE={ M | U }

XLEVEL: Type of Database Cross-Level Security Checking

Parameter	Description	Syntax
XLEVEL	The type of database cross-level security checking to be performed. ■ 0: no cross-level checking ■ 1: Perform a cross-level check only on a user's first call to a database nucleus ■ 2: Perform a cross-level check every time a standard check is performed; this option may be useful if only certain files in the database should be accessible to a particular job ■ 3: The User ID of the originating job should form part of the resource profile name. This option may be useful when different users have different access requirements, depending on the environment in which they are running For more information, see the section Cross-Level Checking.	XLEVEL={0 | 1 | 2 | 3 }

Overriding Parameters Using DDSAF Data Set

Some SAFCFG parameters can be overridden on a nucleus-by-nucleus basis by providing them in a dataset referenced by the DD name DDSAF, thereby avoiding the need to maintain a separate parameter module for each database with different requirements.

The DDSAF dataset should be defined with record size (LRECL) 80 and format fixed (RECFM=F) or fixed-blocked (RECFM=FB), in which case it should have a suitable blocksize.

Each record in DDSAF must begin in column 1, with an asterisk (*) to indicate that it is a comment, or with the parameter keyword and value and optional comments. Each parameter must be specified in a separate record.

The DDSAF dataset is only used for nucleus jobs.

The parameters that can be specified are:

AAFPRFX	LOGOFF
ABS	MAXFILES
ADASCR	MAXPCC
ALLFILES	NOTOKEN
CIPHER	PASSWORD
ETDATA	PCPROT
FAILMODE	REMOTE
FILETAB	XLEVEL
HOLDCMD	

Note: The only valid setting for FAILMODE is FAILMODE=F. This can be used to switch a nucleus running in WARN mode into FAIL mode by modifying DDSAF and restarting ADASAF using ADASAF Online Services (option 6) or by using the AAF SNEWCOPY operator command. FAILMODE=F may only be specified in DDSAF; if specified in the configuration module, it is ignored.

Example

A sample parameter file is shown below:

ADASCR=N	no ADASCR compatibility
CIPHER=Y	some cipher codes
ETDATA=N	no ET data protection
MAXFILES=20	maximum cached files
MAXPC=10	maximum cipher codes
PASSWORD=N	no passwords
XLEVEL=2	full cross-level checking

Daemon Parameters Specified in Configuration Module SAFCFG

This section describes the site-dependent parameters which are used by the SAF Security daemon. These parameters are specified using an assembled configuration module SAFCFG. SAFCFG is supplied as part of the SAF Security Kernel on the Adabas limited libraries.

Note: The default value for each ADASAF parameter is underlined in the parameter syntax definition.

- SAFPRINT: Security Check Trace Message Printing

DBCLASS: ADASAF Resource Class Name

Parameter	Description	Syntax
DBCLASS	The name of the ADASAF resource class. The name can be up to eight alphanumeric characters. This class is used for protection of SYSAAF and other Natural libraries.	DBCLASS={ name | ADASEC} ↩

DBNCU: Number of ADASAF Checks to be Buffered Per User

Parameter	Description	Syntax
DBNCU	The number of security checks to be buffered per SAF user, in the cache defined by GWSIZE. For the security service in the System Coordinator daemon, DBNCU specifies the number of SYSAAF (etc) checks to be buffered per SAF user. These buffered checks are used to avoid repeated SAF calls for a user.	DBNCU=0

DBUNI: Allow Access to Undefined ADASAF Resources

Parameter	Description	Syntax
DBUNI	Indicates whether or not access to undefined resources should be allowed. The normal mode of operation is to prevent access to resources not defined to the security system. Profiles representing ADASAF resources are added to the security repository with either a default access or by granting access to specific users and groups. ■ N: access to undefined resources is not allowed ■ Y: access to undefined resources is allowed **Note:** 1. This option does not permit access to resources defined with universal access "none". 2. DBUNI is ignored when checking whether a nucleus or utility is allowed to execute.	DBUNI={N| Y ↩ }

FAILMODE: Disallow or allow access for security violations

Parameter	Description	Syntax
FAILMODE	FAILMODE controls whether a security violation is treated as "access denied" or "access allowed". ■ F: access is not allowed for security ■ W: access is allowed, even though the security system returned a violation The normal mode of operation is to disallow access for security violations. However, during initial implementation of the security service in the System Coordinator daemon it may be useful to specify FAILMODE=W and, if appropriate, DBUNI=Y so that you can review your SYSAAF (etc) security requirements progressively until you decide to then switch to full fail mode.	FAILMODE={F ↩ | W}

GWMSGL: Trace Level for Daemon Security Checking

Parameter	Description	Syntax
GWMSGL	The tracing level for daemon security checks. ■ 0: no tracing ■ 1: trace violations only ■ 2: trace successful checks only ■ 3: trace all checks For easier problem diagnosis and auditing, trace messages include a time stamp and the name of the job that requested the security check. Trace information is also accumulated in the System Coordinator trace facility, if active.	GWMSGL={ 0 | 1 | 2 ↩ | 3 } ↩

GWSIZE: Storage Size for Caching User Information

Parameter	Description	Syntax
GWSIZE	The amount of storage (in kilobytes) to be used for caching user information related to the security system, for example checked entity names. For optimum performance of the security service in the System Coordinator daemon set GWSIZE large enough so the number of Active SAF User overwrites is not excessive.	GWSIZE=256

GWSTYP: Adabas SAF Security Type

Parameter	Description	Syntax
GWSTYP	The SAF security type. ■ 1: RACF ■ 2: CA-Top Secret ■ 3: CA-ACF2 ■ 4: RACF executing on a Fujitsu operating system.	GWSTYP={ 1 | 2 | 3 | 4 }

SAFPRINT: Security Check Trace Message Printing

Parameter	Description	Syntax
SAFPRINT	Specify whether security check trace messages should be written to DD SAFPRINT or to DD DDPRINT. ■ N: security check trace messages are to be written to DD DDPRINT ■ Y: security check trace messages are to be written to DD If SAFPRINT=Y is specified, but a SAFPRINT dataset is not provided, the trace messages will be written to DDPRINT. The SAFPRINT dataset must be defined in the daemon JCL and may refer to a SYSOUT dataset or to a file defined with RECFM=F (or FB) and LRECL=121.	SAFPRINT={N | Y }