Administrator Services

The Administrator Services subsystem of Natural Security provides the following functions which are used in conjunction with Natural SAF Security:

- NSF Options
- Environment Profiles
- SAF Online Services

In order to use these functions:

- you need to have access to the Natural Security library SYSSEC;
- you have to be defined in Natural Security as a user of type "Administrator";
- you need to have access to the Administrator Services subsystem of Natural Security (as described in the section *Access to Administrator Services* of the *Natural Security* documentation).

Warning:
The user ID "DBA" should not be used for testing purposes. If you log on to SYSSEC as user "DBA", any Natural SAF Security settings and checks will be ignored. As indicated in the *Natural Security* installation documentation, the user ID "DBA" should only be used for the initial definition of Natural Security administrators and for recovering the Natural Security environment.

NSF Options

Natural Security's "General Options" provide several additional options which are used in conjunction with Natural SAF Security to setup your security environment. These "NSF options" are only available if Natural SAF Security is installed.

For any changes of these options to take effect, you have to restart the SAF server and then restart your Natural session.

To invoke the NSF options:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu 1 will be displayed.
2. On the Administrator Services Menu 1, select "General options". The first General Options screen will be displayed.
3. General Options consists of four screens. With PF7 and PF8, you can switch between the screens. General Options 3 and 4 contain the NSF options.

The following types of NSF options are available:

- Security System
- User Options
- NSC Support of RACF
- Environment Options
- Library Options
- RPC Options
- User-Resource Options

The individual options are described below.

General Options 3 (NSF):

```
14:56:35                    *** NATURAL SECURITY ***                2008-08-31
                          - General Options 3 (NSF) -          Server Id 26580

                                          Created ... 2006-09-01 by ADE
                                          Modified .. 2008-08-29 by ADE

 Security System
   External Security System ... RACF     Server ID ............. 26580
   Natural Security ........... FSEC     Protection Level ...... 2


 User Options
   NSF *GROUP ................. Y (Y,N)  NSC Group ID .......... Y (Y,N)
   NSF *USER-NAME ............. Y (Y,N)  NSC User ID ........... N (Y,N)
   NSF *ETID .....(N,O,B,A,J,T) N        NSC Logon Priv.Library  N (Y,D,N)
   NSF *USER Automatic Logon .. N (Y,N)      resource priv.lib.  *USER

NSC Support of RACF
   NSC User Maintenance ....... N (Y,N,X)
   Password case-sensitive .....N (Y,N)


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help        Exit        Def.  Flip  NSC   NSF2                   Canc
```

Security System

Option	Explanation
External Security System	In this field, you specify the external security system to be used. Possible values are: RACF, ACF2 (= CA-ACF2) and TOPS (= CA Top Secret) and SAF. The default value is "SAF": this means that only NSF Options which apply to all supported external security systems are evaluated, while those which are specific to a certain security system will be ignored. **Note:** The value of this option is evaluated internally by Natural SAF Security only, but is not communicated to the SAF server. In the SAF server, the external security system is specified in the configuration module.
Server ID	In this field, you specify the node ID of the SAF server to be used (that is, the value of the parameter GWDBID as specified in the SAF server installation).
Natural Security	*This field is reserved for future use. At present, it must contain "FSEC".*
Protection Level	This field is used to activate Natural SAF Security. Possible values are: **1** - Natural SAF Security is not active, and the SAF server is not accessed. Access to the Natural session is controlled by Natural Security. **2** - Natural SAF Security is active. Access to the Natural session is controlled by the SAF server. *Within* the session, Natural Security determines what users are allowed to do.

User Options

Option	Explanation
NSF *GROUP	Determines whether the group ID defined in the external security system is to be used as value for the Natural system variable *GROUP (Y/N). It is recommended that this option be set to "Y" (see also option "NSC Group ID" below).
NSC Group ID	Determines whether the group IDs defined in the external security system also have to be defined in Natural Security (Y/N). It is recommended that this option be set to "Y"; any conditions of use associated with the Natural Security group profile can then be controlled by Natural Security. RACF allows for a user to be in multiple groups. If this option is set to "Y", any of these groups can be used for a logon to a protected library, and they will be evaluated by the Natural logon procedure to select the group to be used for the logon.
NSF *USER-NAME	Determines whether the user name defined in the external security system is to be used as value for the Natural system variable *USER-NAME (Y/N).

Option	Explanation
NSC User ID	Determines whether, in addition to being defined in the external security system, users also have to be defined in Natural Security (Y/N). If set to "Y", the Natural Security user profile will be used once the user has successfully logged on to the external security system. After the initial logon, the conditions of use associated with the Natural Security user profile will be controlled by Natural Security. However, Natural Security will not perform any password checks.
NSF *ETID	Determines if and how ETIDs (end of transaction IDs) are to be generated by Natural SAF Security at the start of the Natural session: **N** No ETIDs are generated by Natural SAF Security; they are generated by Natural Security. **O** Generate ETIDs only for online users. **B** Generate ETIDs only for batch-mode users. **A** Generate ETIDs for all (online and batch-mode) users. **J** Use the job name as ETID (for batch-mode users only). **T** Use the value of the Natural system variable *INIT-ID as ETID.
NSC Logon Priv. Library	This option controls users’ access to private libraries: **N** Access to private libraries is controlled by Natural Security. **Y** When a user logs on without specifying a library ID, the current value of the Natural system variable *USER will be used as library ID. If the library option "Protect Libraries" (see below) is set, this requires a corresponding resource profile for this library. **D** When a user logs on without specifying a library ID, the current value of the Natural system variable *USER will be used as library ID. If the library option "Protect Libraries" (see below) is set, this requires a corresponding resource profile for the value specified as "Resource priv. lib." (see below). Access validation in the external security system will be based on this value (instead of the value of the system variable *USER). If this option is set to a value other than "N", the library option "Protect Libraries" (see below) must also be set to a value other than "N".
Resource priv. lib.	Only applicable if "NSC Logon Priv. Library" (see above) is set to "D": In this field, you specify the value which is to be used for access validation to private libraries. This value applies to all users. The default value is the string "*USER".

Option	Explanation
NSF *USER Automatic Logon	When Automatic Logon is used (Natural profile parameter AUTO=ON), Natural uses the value of the Natural system variable *INIT-USER as value for the Natural system variable *USER. To prevent this, you can use this option. **Y** The *INIT-USER value is not used for *USER. **N** The *INIT-USER value is used for *USER (this is the default).

NSC Support of RACF

These options are only available if RACF is used as the external security system.

Option	Explanation
NSC User Maintenance	This option allows you to change user passwords in RACF user profiles, with the base segment field keyword EXPIRED, from within Natural Security's user maintenance. Before this option can be used, the subprogram NSFRACF1, whose source is supplied in the library SYSSEC, has to be cataloged in SYSSEC under the name NSCNRACF. The source is made available for you to see its highly sensitive functioning. You need not make any changes to it, but can catalog it as it is. If necessary, however, you may adjust it to suit your requirements. Using this option/subprogram requires that in RACF you have the appropriate authorizations. That is, you can only set the RACF user passwords and EXPIRED base segment field keywords via Natural Security if you are allowed to do so in RACF itself. Setting this option to "Y" causes the following changes on Natural Security user profile screens: ● Instead of the user name as defined in Natural Security, the user name as defined in the RACF user profile is displayed. ● Instead of the fields New Password and Change After *nnn* Days, the field RACF Password is displayed. If you enter a password in that field, this will cause the user's password as defined in the *RACF* user profile to be changed accordingly. To set the *Natural Security* user password, you press PF9. Setting this option to "X" has the same effects as "Y". In addition, it causes a check to be performed as to which user IDs defined in Natural Security are also defined in RACF. As a result, the user IDs defined in both systems will be marked accordingly on Natural Security's User Maintenance selection list.

Option	Explanation
Password Case-Sensitive	This option is relevant if RACF is set to distinguish between lower-case and upper-case characters in user passwords. It determines whether or not this distinction is to be made by Natural SAF Security as well: • N - Natural SAF Security internally converts all alphabetical characters in passwords to upper-case. • Y - Natural SAF Security distinguishes between lower- and upper-case characters in passwords. If you set this option to "Y", the option "Password Case-Sensitive" in Natural Security's *Library and User Preset Values* is automatically set to "Y" as well to ensure consistent password checking. If you set this option to "Y", make sure that any password input fields used also distinguish between lower- and upper-case. This may affect the logon screen, the user exit LOGONEX1, any logon-related Natural Security application programming interfaces, or Natural's RPC-logon-related application programming interfaces.

General Options 4 (NSF):

```
13:45:37                    *** NATURAL SECURITY ***                2008-08-31
                          - General Options 4 (NSF) -          Server Id 26580

                                                Created ... 2006-09-01 by ADE
                                                Modified .. 2008-08-18 by ADE

 Environment Options
  Protect Environments ....... N (Y,N)   Allow Undef. Environments .. N (Y,N)

 Library Options
  Protect Libraries .......... N (Y,L,R,*,N) with Environment ....... N (Y,N)
  Disable Natural Commands ... N (Y,N)   Set FUSER Read-Only ........ N (Y,N)
  Protect Natural Modules .... N (Y,X,N)

 RPC Options
  Protect Services ........... N (Y,F,N)     with Environment ....... N (Y,N)

 User-Resource Options
  with Environment ........... N (Y,N)   Allow Undef. Resources ..... N (Y,N)



Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help        Exit        Def.  Flip  NSF1                          Canc
```

Environment Options

Option	Explanation
Protect Environments	Determines whether the environment profile of the system-file combination (FNAT, FUSER, FDIC, FSEC) is to be checked at the logon (Y/N). **Y** The access level defined for the environment in the external security system determines whether a user has access to it or not. **N** Users have access to any environment. See also *Environment Profiles* below.
Allow Undef. Environments	Determines whether undefined system-file combinations are to be accepted at the logon (Y/N). This option is only relevant if RACF is used as external security system. With other external security systems, this option will be ignored.

Library Options

Option	Explanation
Protect Libraries	Determines whether the library access level is to be checked via the SAF server: **Y** To log on to a library, users need at least READ access to the library and all steplibs defined for that library. **L** To log on to a library, users need at least READ access to the library (but not to the steplibs). **R** If RACF is used as external security system, you can set this option to "R": The library access level will be checked, but access to libraries not defined in RACF will also be possible. The access level of the library and its steplibs will be checked. ***** This is the same as "R", except that only the access level of the library itself (but not of the steplibs) will be checked. **N** Access to libraries is controlled by Natural Security according to the Natural Security logon rules. "R" and "*" only apply with RACF. For other security systems, they are not possible. If this option is set to a value other than "N", the user option "NSC Logon Priv. Library" (see above) must also be set to a value other than "N".
with Environment	Determines whether the environment alias is to be used as prefix of the resource library for the access-level check (Y/N). See also *Environment Profiles* below.

Option	Explanation
Disable Natural Commands	Determines whether the use of Natural system commands is to be controlled by the access level (Y/N). If this option is set to "Y", the access level determines whether the use of Natural system commands is allowed: ● If the access level is CONTROL or higher, the use of system commands is allowed. ● if the access level is lower than CONTROL, the use of system commands is not allowed. If this option is set to "Y", the Natural profile parameter NC as well as any settings concerning system commands in Natural Security library profiles (Allow System Commands, Command Restrictions and Editing Restrictions) will be ignored.
Set FUSER Read-Only	Determines whether read-only access to the FUSER system file is to be controlled by the access level (Y/N). If this option is set to "Y", the access level determines whether modifications of the data on the FUSER system file are allowed: ● If the access level is ALTER, modifications on the FUSER file are allowed. This requires the definition of a Natural scratch-pad file (as described in the Natural *Operations* documentation for mainframes). ● If the access level is lower than ALTER, modifications on the FUSER file are not allowed. If this option is set to "Y", the RO option of the Natural profile parameter FUSER is ignored.
Protect Natural Modules	Determines whether the execution of Natural programming objects is to be controlled by the external security system: **Y** It is checked whether a programming object may be executed for the current library (as determined by the Natural system variable *LIBRARY-ID). **X** It is checked whether a programming object may be executed in the library in which it is stored. **N** Execution permission is controlled by the Natural Security library profile containing the programming object. An example of the effects of this option is shown under Programming Objects > Natural SAF Security Definitions. The use of this option requires that certain Natural profile parameters be set; see Step 2 of the installation procedure.

RPC Options

Option	Explanation
Protect Services	Determines if the Natural RPC service access is to be checked via the SAF server (N/Y/F): **N** Access to a service is controlled by the Natural Security library profile of the library containing the subprogram. **Y** Access to a service is controlled by the resource profile. Users need at least READ access to execute a service. In addition, the library profile of the library containing the subprogram applies. Access to services not defined in RACF is also possible. **F** This is the same as "Y", except that access to services not defined in RACF is not possible. "Y" and "F" are only different for RACF; for other security systems, "F" has the same effect as "Y".
with Environment	Determines whether the environment alias is to be used for the service-access check (Y/N). See also *Environment Profiles* below.

User-Resource Options

Option	Explanation
with Environment	Determines whether the environment alias is to be used as prefix to the resource definitions (Y/N). See also *Environment Profiles* below.
Allow Undef. Resources	Determines whether access to undefined resources is to be allowed via the Natural SAF Security application programming interfaces (Y/N). This option is only relevant if RACF is used as the external security system. With other external security systems, this option will be ignored.

Environment Profiles

If you wish to protect resources in specific environments, you have to define environment profiles for these environments (that is, security profiles for the individual system-file combinations).

In an environment profile, you specify a one-character alias for the environment. The alias is used to identify the environment to the external security system; the environment-specific resource profiles whose names are prefixed with this alias determine users’ access rights, if the "with Environment" option for the resource class in question is set to "Y" in the NSF options (see above).

To define environment profiles, you use the Natural Security function "Environment Profiles", as described under *Defining Environment Profiles* in the section *Protecting Environments* of the *Natural Security* documentation.

For any environment-profile modifications to take effect in Natural SAF Security, you have to restart your Natural session.

SAF Online Services

SAF Online Services provide several functions for monitoring the SAF server. They are described under *SAF Online Services* in the *Natural Security* documentation.

SAF Online Services can be invoked:

- from within the Natural Security library SYSSEC by selecting it from the Administrator Services Menu, or
- from anywhere else in Natural by issuing the direct command SYSSAFOS.

To be able to access SAF Online Services, a utility security profile for SYSSAFOS has to be defined in Natural Security (as described in the section *Protecting Utilities* of the *Natural Security* documentation).