

# Administrator Services

If Natural SAF Security is installed, the Administrator Services subsystem of Natural Security provides the following additional functions, which are used in conjunction with Natural SAF Security:

- General NSF Options
- Definition of System-File Environments
- NSF Online Services

In order to perform these Natural SAF Security functions, you need to have access to the Natural Security library SYSSEC. Also, you have to be defined in Natural Security as a user of type "Administrator". Moreover, you need to have access the Administrator Services subsystem of Natural Security (as described in the section Access to Administrator Services of the Natural Security documentation).

**Note:**

Be careful when using the user ID "DBA": 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.

---

## General NSF Options

This function is used to set various Natural SAF Security options.

For any changes of these options to take effect, you have to restart your Natural session.

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 1, select "Set general options". The Set General Options screen will be displayed.
3. Press PF8 (NSF1). The General NSF Options screen will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.

## General NSF Options - Screen 1

On the first General NSF Options screen, you can set the following options:

### Security System

Option	Explanation
<b>Ext. Sec. System</b>	<p>In this field, you specify the external security system to be used.</p> <p>Possible values are: RACF, ACF2 (= CA-ACF2) and TOPS (= CA Top Secret) and SAF.</p> <p>The default value is "SAF": this means that only General 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.</p> <p><b>Note:</b> 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.</p>
<b>Server ID</b>	<p>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).</p>
<b>Natural Security</b>	<p><i>This field is reserved for future use. At present, it must contain "FSEC".</i></p>
<b>Protection Level</b>	<p>This field is used to activate Natural SAF Security. Possible values are:</p> <p><b>1</b> - Natural SAF Security security is not active, and the SAF server is not accessed. Access to the Natural session is controlled by Natural Security.</p> <p><b>2</b> - Natural SAF Security security is active. Access to the Natural session is controlled by the SAF server. <i>Within</i> the session, Natural Security determines what users are allowed to do.</p>

## User Options

Option	Explanation
<b>NSF *GROUP</b>	<p>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).</p> <p>It is recommended that this option be set to "Y" (see also option "NSC Group ID" below).</p>
<b>NSC Group ID</b>	<p>Determines whether the group IDs defined in the external security system also have to be defined in Natural Security (Y/N).</p> <p>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.</p>
<b>NSF *USER-NAME</b>	<p>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).</p>
<b>NSC User ID</b>	<p>Determines whether, in addition to being defined in the external security system, users also have to be defined in Natural Security (Y/N).</p> <p>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.</p>
<b>NSF *ETID</b>	<p>Determines if and how ETIDs (end of transaction IDs) are to be generated by Natural SAF Security at the start of the Natural session:</p> <p><b>N</b> No ETIDs are generated by Natural SAF Security; they are generated by Natural Security.</p> <p><b>O</b> Generate ETIDs only for online users.</p> <p><b>B</b> Generate ETIDs only for batch-mode users.</p> <p><b>A</b> Generate ETIDs for all (online and batch-mode) users.</p> <p><b>J</b> Use the job name as ETID (for batch-mode users only).</p> <p><b>T</b> Use the value of the Natural system variable *INIT-ID as ETID.</p>
<b>NSC Logon Priv. Library</b>	<p>Determines whether users are to be able to access other users' private libraries (provided the external security system allows this) (Y/N).</p>

## General NSF Options - Screen 2

On the second General NSF Options screen, you can set the following options:

### Environment Options

<b>Option</b>	<b>Explanation</b>
<b>Protect Environments</b>	<p>Determines whether the environment profile of the system-file combination (FNAT, FUSER, FDIC, FSEC) is to be checked at the logon (Y/N).</p> <ul style="list-style-type: none"><li>● If this is set to "Y", the access level defined for the environment in the external security system determines whether a user has access to it or not.</li><li>● If this is set to "N", users have access to any environment.</li></ul> <p>See also Definition of System-File Environments below.</p>
<b>Allow Undef. Environments</b>	<p>Determines whether undefined system-file combinations are to be accepted at the logon (Y/N).</p> <p>This option is only relevant if RACF is used as external security system. With other external security systems, this option will be ignored.</p>

## Library Options

Option	Explanation
<b>Protect Libraries</b>	<p>Determines whether the library access level is to be checked via the SAF server (Y/N/R).</p> <ul style="list-style-type: none"> <li>● Y - Users need at least READ access to log on to a library.</li> <li>● N - Access to libraries is controlled by Natural Security according to the Natural Security logon rules.</li> <li>● 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. For other security systems, "R" is not possible.</li> </ul>
<b>with Environment</b>	<p>Determines whether the environment alias is to be used as prefix of the resource library for the access-level check (Y/N).</p> <p>See also Definition of System-File Environments below.</p>
<b>Disable Natural Commands</b>	<p>Determines whether the use of Natural system commands is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether the use of Natural system commands is allowed:</p> <ul style="list-style-type: none"> <li>● If the access level is CONTROL or higher, the use of system commands is allowed.</li> <li>● If the access level is lower than CONTROL, the use of system commands is not allowed.</li> </ul> <p>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.</p>
<b>Set FUSER Read-Only</b>	<p>Determines whether read-only access to the FUSER system file is to be controlled by the access level (Y/N).</p> <p>If this option is set to "Y", the access level determines whether modifications of the data on the FUSER system file are allowed:</p> <ul style="list-style-type: none"> <li>● 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).</li> <li>● If the access level is lower than ALTER, modifications on the FUSER file are not allowed.</li> </ul> <p>If this option is set to "Y", the RO option of the Natural profile parameter FUSER is ignored.</p>

## RPC Options

Option	Explanation
<b>Protect Services</b>	<p>Determines if the Natural RPC service access is to be checked via the SAF server (Y/N).</p> <p>If you specify "N", only the service access is checked.</p> <p>If you specify "Y", the service access and the Natural Security library profile are checked.</p>
<b>with Environment</b>	<p>Determines whether the environment alias is to be used for the service-access check (Y/N).</p> <p>See also Definition of System-File Environments below.</p>

## User-Resource Options

Option	Explanation
<b>Allow Undef. Resources</b>	Determines whether access to undefined resources is to be allowed via the Natural SAF Security user exits (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.
<b>with Environment</b>	Determines whether the environment alias is to be used as prefix to the resource definitions (Y/N).  See also Definition of System-File Environments below.

## Definition of System-File Environments

This function is used to define environment profiles, that is, security profiles for the individual system-file combinations.

If you wish to protect resources in specific environments, you have to define environment profiles for these environments. In an environment profile, you specify a one-character alias for the environment. The alias is used 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 General NSF Options (see above).

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

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 2, select "Definition of System-File Environments". The Define System-File Environments screen will be invoked.

### Define System-File Environments Screen

The Define System-File Environments screen displays a list of all environment profiles which have been defined.

For each environment profile, its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT), name, alias (AL) and protection status (P) are displayed. The protection status can be:

<b>I</b>	The environment profile is inactive (both NSC and NSF Protection = N in the environment profile) .
<b>N</b>	The environment is only evaluated by Natural Security (NSC Protection = Y in the environment profile).
<b>S</b>	The environment is only evaluated by the SAF server (NSF Protection = Y in the environment profile).

### Available Functions

The following functions are available:

Code	Function
<b>AD</b>	Add new environment profile. (You can also invoke this function by entering "AD" in the Command line.)
<b>MO</b>	Modify environment profile.
<b>DE</b>	Delete environment profile.
<b>DI</b>	Display environment profile.

To invoke a function for an environment, you mark the environment with the appropriate function code in column "Co".

## Components of an Environment Profile

When you add a new environment or modify an existing one, the Define Environment Profile screen will be displayed. The items you can define as part of an environment profile on this screen and any subsequent screens/windows are:

Field	Explanation
<b>Environment Name</b>	You can specify a descriptive name for the environment profile.
<b>Alias</b>	You specify a one-character alias for the environment profile. This alias is used in the external security system to define the resources related to the system-file combination of this environment.  It is possible for multiple environment profiles to share the same alias. The rules defined for an alias in the external security system apply to all system-file combinations in whose environment profiles this alias is specified.
<b>General Options</b>	You specify the protection status of the environment:  <b>NSF Protection</b> - If set to "Y", this activates the environment for validation by the SAF server - provided that the option "Protect Environment" in the General NSF Options (see above) is set to "Y".  <b>NSC Protection</b> - If set to "Y", this activates the environment for validation by Natural Security.  If both are set to "N", the environment is not evaluated. It is not possible to set both to "Y".
<b>System Files</b>	You define the environment by specifying the database IDs and file number of each system file (FUSER, FDIC, FSEC, FNAT). This combination of system files identifies the environment and must be unique.  Once entered, the values of these fields cannot be changed.

## Additional Options

If you either mark the field "Additional Options" with "Y" or press PF4, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

They correspond to the options of the same names in Natural Security library profiles, as described in the Natural Security documentation.

## NSF Online Services

Before you can use NSF Online Services, you have to define a utility security profile for the utility SYSNSFOS (which contains the NSF Online Services) in Natural Security.

NSF Online Services provides several functions for monitoring the SAF server.

To invoke this function:

1. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed. It consists of two screens. With PF7 and PF8, you can switch between the two screens.
2. On the Administrator Services Menu 2, select "NSF Online Services".

The Online Services menu will be displayed. It provides the following functions:

- System Parameters
- System Statistics
- User Statistics
- Zap Maintenance
- Storage Display
- System Tracing
- Server Restart

## System Parameters

This function display the parameter settings as defined in the system parameter module. The following information is displayed:

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server that are related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Class/Type	Shows the names of the different SAF general resources Classes or Types. These contain either the default or any override values which have been defined in the system parameter module.
Universal	This indicates a particular check is designated universal. If selected, then failure to define a particular resource profile will result in all users having access to it. Natural Program execution authorization cannot be designated universal.
Buffered	Displays for each type of check the maximum number of positive checks that the SAF server can buffer on behalf of each user.
Logging	This indicates the SMF logging level required when performing security checks. "0" signifies logging ASIS, that is, in accordance with the default for the security Class/Type; "1" indicates an override setting of NONE.
Active	Designates the particular authorization checks that are active. This applies only to checks performed by mainframe Natural as all other checks are activated by the installation process.
Env (Environment)	Indicates that an environment code, based on the Natural system files, is used to prefix certain resource profiles. Applies only to authorization checks performed by mainframe Natural.

Storage (k)	The size of the buffer in kilobytes which can be used for caching positive security checks in the address space of the SAF server.
Server DBID	Shows the database ID used by the SAF server.
Encrypt Req.	Indicates whether security requests passed between different SAF server components are communicated encrypted.
Encrypt Stg.	Indicates whether storage maintained within the Natural environment is kept in an encrypted state.
Messages	SAF server message level: Level "0" gives only error message, "1" reports security violations and "3" generates an audit trail of all checks.
Cmd Log	Indicates whether command logging is turned on.
Buffer	Indicates whether security checks will be cached by the SAF server.
JCL check	Indicates whether CA-JCL check processing is available within the Natural environment.
Prefix Prog	Indicates whether Natural program names are prefixed with the name of the current application library when performing authorization checks. <i>Not applicable to Natural SAF Security.</i>
Protect Obj	Indicates whether program objects are protected within the Natural environment. Users require ALTER access to a particular application in order to modify its program objects. <i>Not applicable to Natural SAF Security.</i>
Log SYSMAIN	Indicates whether logging of all SYSMAIN operation is required. <i>Not applicable to Natural SAF Security.</i>
SYSMAIN/Lib	Indicates whether authorization checks for SYSMAIN functions will include access to the relevant Natural application libraries. <i>Not applicable to Natural SAF Security.</i>
Cmd Line	Indicates whether the Natural command line is protected. Users require CONTROL access in order to enter commands in the Natural command line.
ETID	Indicates whether Natural will generate a unique ETID.
Edit/Lib	Indicates whether Natural will prevent editing of objects located in another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Clear/Ed	Indicates whether Natural will clear the edit area when logging onto another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Ext Name	Indicates whether Natural will take the user name from SAF. Specifically, the field *USER-NAME will be taken from RACF or CA-ACF2.
Ext Group	Indicates whether Natural will take the group name from SAF. That is, the field *GROUP will be taken from RACF, CA Top Secret, CA-ACF2.
Log API	Indicates whether SMF logging is performed when executing the Natural API.
Env API	Indicates whether authorization checks performed by the Natural API will be prefixed by an environment code based on the Natural system files.

## System Statistics

This function displays statistical information on the SAF server. The following information is displayed:

<b>Item</b>	<b>Explanation</b>
Authorization	Displays the different resource authorization checks performed by the SAF server related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Check (+ve)	Indicates the number of authorization checks performed against the security system for each check type. The count indicates authorizations for which access was permitted and can include universal checks.
Check (-ve)	Indicates the number of authorization checks performed against the security system for which access was denied.
Check saved	Shows the number of authorization checks that were optimized by the SAF server because the result was already known.
Overwritten	Number of times positive authorization results were overwritten in the SAF server's cache because more recent information took its place in the buffer. Increase the number of items buffered if this count is excessive for any particular check type.
Lngh	Number of bytes reserved to cache resource profiles belonging to each type of authorization check. This value is generated automatically by the system.
Active Users	Number of users currently active in the SAF server.
High Watermark	High watermark value for number of users present in the SAF server.
Max Users	Maximum of users that can be accommodated.
Overwritten	Number of times a user area was reclaimed and allocated to another user. Increase the total buffer size if this count becomes excessive.
Authenticated	The total number of successful authentication checks performed.
Denied	The number of unsuccessful authentication checks.

## User Statistics

This function displays statistical information on the currently active users. The function displays a list of users. When you select a user from the list, statistical information on this user will be displayed. The individual items correspond to the items of the same names as described above for System Statistics.

## Zap Maintenance

This function displays a list ZAPs applied to the SAF server.

## Storage Display

This function displays the storage of the SAF server's address space.

## System Tracing

This function displays a list of the 256 most recent trace events.

## Server Restart

This function is used to restart the SAF server. The Restart function ensures that all data held in the SAF server's own buffer are flushed. In addition, any data held by the security system itself in the address space of the SAF server are flushed by this action.

