

Protecting Environments

This section covers following topics:

- Concept of Environment Protection
 - Activation of Environment Protection
 - Defining Environment Profiles
 - Components of an Environment Profile
 - Disallowing/Allowing Access to Libraries in Environments
 - Disallowing/Allowing Users Access to Environments
-

Concept of Environment Protection

Natural Security allows you to make users' access to a library environment-specific. A Natural *environment* is determined by the combination of the system files FNAT, FUSER, FSEC and FDIC. You define a security profile for each environment (that is, for each system-file combination) you wish to protect, and control users' access to it. You can also make a library accessible in some environments, but not in others.

A logon to another environment occurs when a users logs onto a library located on another FUSER system file (as specified by the "Library File" DBID/FNR in the library profile).

Whenever a user logs on to a library in another environment, Natural Security will check whether:

- access to the library is allowed in that environment, and
- the user is authorized to access that environment.

Such a check is performed not only when a user explicitly logs on to a library, but also when the user invokes a function which implicitly accesses another library or processes the contents of another library.

Activation of Environment Protection

Environment protection is activated by setting the general option "Environment Protection" to "Y".

If environment protection is active, the following applies:

- Access to undefined environments is not possible.
- For every environment to be accessed, an environment security profile has to be defined.
- By default, access to a library is allowed in any defined environment.
- By default, access to a defined environment is allowed for all users.
- For individual defined environments, you can disallow access to a library.
- For individual users, you can disallow access to a defined environment.

To deactivate environment protection, you set the general option "Environment Protection" option to "N".

Defining Environment Profiles

The Administrator Services function "Environment Profiles" is used to define environment profiles, that is, security profiles for the individual system-file combinations.

To invoke this function, you select "Administrator Services" on the Main Menu. The Administrator Services Menu will be displayed.

Note:

Access to Administrator Services may be restricted (as explained in the section Administrator Services).

On the Administrator Services Menu 2, you select "Environment profiles". The Environment Maintenance selection list will be invoked.

Environment Maintenance Selection List

The Environment Maintenance selection list displays a list of all environment profiles which have been defined.

The list can be scrolled as described in the section Finding Your Way In Natural Security.

For each environment profile, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed.

Protection Status

The protection status can be:

I	The environment profile is inactive (both NSC Protection = N and NSF Protection = N in the environment profile).
N	Access to the environment is evaluated by Natural Security (NSC Protection = Y in the environment profile).
S	Access to the environment is evaluated by the SAF server (NSF Protection = Y in the environment profile).

Available Functions

The following functions are available:

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

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

You may select various environments for various functions at the same time; that is, you can mark several environments on the screen with a function code. For each environment marked, the selected functions will then be executed one after another.

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
Environment ID	You specify a descriptive name for the environment profile.
Alias	<p>You can specify a one-character alias for the environment profile. An alias can be shared by multiple environment profiles. By specifying the same alias in several environment profiles, you can form groups of environments.</p> <p>For example, you can use aliases like: D - for all development environments, T - for all test environments, P - for all production environments.</p> <p>This will make the maintenance of environment profiles easier, because you can use the alias as selection criterion on the Environment Maintenance selection list to list all profiles which have the same alias.</p> <p>For Natural SAF Security the following applies: The alias is used in the external security system to define the resources related to the system-file combination of this environment. 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.</p>
General Options	<p>You specify by which system the environment is to be protected:</p> <p>NSC Protection - If set to "Y", this activates the environment for validation by Natural Security, as described in this documentation.</p> <p>NSF Protection - If set to "Y", this activates the environment for validation by the SAF server, as described in the Natural SAF Security documentation. This validation requires that the option "Protect Environment" in the General NSF Options is set to "Y" (see Natural SAF Security documentation).</p> <p>If both are set to "N", the environment profile is not active, that is, it is treated as if it were not defined.</p>
System Files	<p>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.</p> <p>Once entered, the values of these fields cannot be changed.</p>

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

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	In this window, the following information is displayed: <ul style="list-style-type: none"> ● the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ● the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this environment security profile or allow/disallow users' access to it. If no owner is specified, any user of type ADMINISTRATOR may do so. For each owner, the number of co-owners whose countersignatures will be required for maintenance/link permission may optionally be specified in the field after the ID. For an explanation of owners and co-owners, see the section Countersignatures.

Disallowing/Allowing Access to Libraries in Environments

By default, when environment protection is active, access to a library is allowed in any environment. For individual environments, you can disallow access to a library.

When access to a library is disallowed in at least one environment, the fact that the library is "environment-protected" will be indicated in the library's security profile.

Two functions are available to disallow/allow environment-specific access to libraries:

- To disallow/allow access to various libraries for one environment, you use the function "Protect environment" (which is invoked from the Environment Maintenance selection list).
- To disallow/allow access to one library for various environments, you use the function "Protect environments" (which is invoked from the Library Maintenance selection list).

Both functions are described below.

Protecting a Single Environment for Multiple Libraries

On the Environment Maintenance selection list, you mark the environment you wish to protect with "EP".

A window will be displayed. Here you enter an "L" in the field "Protect for users/libraries". You can also enter a Start Value (as described in the section Finding Your Way in Natural Security) for the list of libraries to be displayed. In addition, you can select the option "Select only disallowed ones" - in which case the list of libraries to be displayed will only include those libraries for which access in the environment is currently disallowed.

Then, the Disallow/Allow Libraries screen will be displayed, showing the list of libraries. The list can be scrolled as described in the section Finding Your Way In Natural Security.

On the list, you mark the libraries for which you wish to disallow/allow access in the environment.

In the "Co" column, you may mark each library with one of the following function codes:

Code	Function
ED	Disallow - The library cannot be accessed in that environment.
EA	Allow - The library can be accessed in that environment.

You can mark one or more libraries on the screen with a function code. For each library marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each library.

Protecting Multiple Environments for a Single Library

On the Library Maintenance selection list, you mark the library for which you wish to with function code "EP".

A window will be displayed, in which you have the following options:

Option	Explanation
Disallow/allow	<p>D - Access to the library is initially allowed for all environments, and you can disallow it for individual ones.</p> <p>A - Access to the library is initially disallowed for all environments, and you can allow it for individual ones.</p> <p>When you later invoke this function and change the value of this option, the "allowed/disallowed" status of all environments will be changed for this library.</p>
Sorted by environment ID / Sorted by alias	By marking one of these two fields with a character, you can choose to have the list of environments to be displayed sorted by environment IDs or by aliases. The latter allows you to simultaneously allow/disallow access for all environments which have the same alias (see below).
Start value	In one of these two fields, you can enter a start value (as described in the section Finding Your Way in Natural Security) for the list of environments to be displayed. Depending on how the list is to be sorted, you can specify either the database ID / file number of the environments' FNAT system file or a one-character alias as start value.
Select only disallowed/allowed ones	If you select this option, the list of environments to be displayed will only include - depending on the above option "Disallow/allow" - either those for which access is allowed or those for which it is disallowed.

Then, the Disallow/Allow Environments screen will be displayed, showing the list of environments. For each environment, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed. The list can be scrolled as described in the section Finding Your Way In Natural Security.

On the list, you mark the environments for which you wish disallow/allow access to the library.

In the "Co" column, you may mark each environment with one of the following function codes:

Code	Function
ED	Disallow - The library cannot be accessed in that environment.
EA	Allow - The library can be accessed in that environment.

You can mark one or more environments with a function code. For each environment marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each environment.

If the list is sorted by alias, you do not mark individual environments. Instead, you mark an alias, and the selected function will be applied to all environments which have that alias.

Disallowing/Allowing Users Access to Environments

By default, when environment protection is active, access to an environment is allowed for all users. For individual users you can disallow access to an environment.

Access to an environment can only be allowed/disallowed for users of types GROUP, ADMINISTRATOR and PERSON. For users of types ADMINISTRATOR and PERSON it can be allowed/disallowed either directly or via a GROUP. For users of types MEMBER and TERMINAL, it can only be allowed/disallowed for the GROUP to which they are assigned.

When access to at least one environment is disallowed for a user, the session option "Environment Protection" in the user's security profile is automatically to "Y".

Two functions are available to disallow/allow users' access to environments:

- To disallow/allow access of various users to one environment, you use the function "Protect environment" (which is invoked from the Environment Maintenance selection list).
- To disallow/allow access of one user to various environments, you use the function "Protect environments" (which is invoked from the User Maintenance selection list).

Both functions are described below.

Protecting a Single Environment for Multiple Users

On the Environment Maintenance selection list, you mark the environment you wish to protect with "EP".

A window will be displayed. Here you enter a "U" in the field "Protect for users/libraries". You can also enter a Start Value (as described in the section Finding Your Way in Natural Security) for the list of users to be displayed. In addition, you can select the option "Select only disallowed ones" - in which case the list of users to be displayed will only include those users for whom access to the environment is currently disallowed.

Then, the Disallow/Allow Users screen will be displayed, showing the list of users. By default, the list contains only users of type GROUP. To switch between a list of GROUPs and a list of all three user types, you press PF5. The list can be scrolled as described in the section Finding Your Way In Natural Security.

On the list, you mark the users for whom you wish to disallow/allow access to the environment.

In the "Co" column, you may mark each user with one of the following function codes:

Code	Function
ED	Disallow - The user cannot access the environment.
EA	Allow - The user may access the environment

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each user.

Protecting Multiple Environments for a Single User

On the User Maintenance selection list, you mark the user for whom you wish to protect environments with function code "EP".

A window will be displayed. Here you can enter a Start Value (as described in the section Finding Your Way in Natural Security) for the list of environments to be displayed; as start value, you use the database ID / file number of the environments' FNAT system file. You can also select the option "Select only disallowed environments" - in which case the list of environments to be displayed will only include those environments to which access is currently disallowed for the user.

Then, the Disallow/Allow Environments screen will be displayed, showing the list of environments. For each environment, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed. The list can be scrolled as described in the section Finding Your Way In Natural Security.

On the list, you mark the environments the access to which you wish to disallow/allow for the user.

In the "Co" column, you may mark each environment with one of the following function codes:

Code	Function
ED	Disallow - The user cannot access the environment.
EA	Allow - The user may access the environment.

You can mark one or more environments on the screen with a function code. For each environment marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each environment.