

# Defining Resources in the External Security System

This section describes which resources have to be defined in the external security system in conjunction with Natural SAF Security. It covers the following topics:

- Users
- Environments
- Libraries
- RPC Services
- User-Defined Resources
- Overview of Resource-Class Definitions

## Note:

Some external security systems use the term "resource profile", others the term "rule". In this documentation the term "resource profile" is used.

Some external security systems use the term "resource class", others the term "resource type". In this documentation the term "resource class" is used.

---

## Users

No special user-specific definitions have to be made in the external security system.

If the General NSF Options "NSF \*GROUP" and "NSF \*USER-NAME" are set to "Y", the user's group and user name as defined in the external security system are passed to Natural SAF Security.

## Environments

With Natural SAF Security, Natural environments can be protected to prevent unauthorized users from accessing the system files.

A Natural environment is determined by the combination of the Natural system files FNAT, FDIC, FSEC and FUSER. For each system-file combination that is to be protected, a resource profile has to be defined in the external security system. The identification of the resource profile must be a 40-digit number corresponding to the database ID / file number (DBID/FNR) combinations of the four system files. The database IDs and file numbers must be specified in the following sequence:

1) FNAT DBID, 2) FNAT FNR, 3) FDIC DBID, 4) FDIC FNR, 5) FSEC DBID, 6) FSEC FNR, 7) FUSER DBID, 8) FUSER FNR.

Each DBID and FNR must be specified as a 5-digit number (padded with leading zeros).

### Example:

```
0001100035000110003300011000340001100032
```

The above specification would refer to the following environment:

```
FNAT=(00011,00035), FDIC=(00011,00033), FSEC=(00011,00034), FUSER=(00011,00032)
```

The option "Protect Environments" in the General NSF Options determines if access to a Natural environment is to be controlled by Natural SAF Security. If this option 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. A user needs at least READ access to be able to access a Natural environment.

The resource-class name for Natural environments is defined with the macro parameter NACLSE in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSFSAG".

## Libraries

With Natural SAF Security, Natural libraries can be protected to control users' access to them.

You can protect a Natural library:

- independently of the environment, or
- in specific environments.

The resource-class name for Natural libraries is defined with the macro parameter NACLTC in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NTCSAG".

## Environment-Independent Access to a Library

If a Natural library is to be protected, a resource profile has to be defined for it in the external security system.

The resource-profile name must correspond to the library ID and may be up to 8 characters long.

The option "Protect Libraries" in the General NSF Options determines if access to Natural libraries is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for a library in the external security system determines whether a user can log on to the library or not. The access level is checked when a users logs on to a Natural library. A user needs at least READ access to be able to log on to a library.

## Access to a Library in Specific Environments

If a Natural library is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-library combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias and the library ID (up to 8 characters), separated by a period:

*a.library-ID*

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific library-access check is activated by the option "with Environment" in the Library Options section of the General NSF Options. Access to the library is then only possible in environments to which the user has READ access.

## Use of System Commands in a Library

If the option "Disable Natural Commands" in the General NSF Options is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not users may use Natural system commands within the library. If the option is set to "Y", users need at least CONTROL access to use system commands.

## Modifications on FUSER System File

If the option "Set FUSER Read-Only" in the General NSF Options is set to "Y", the access level defined for the library (or library-environment combination) in the external security system also determines whether or not the user may make modifications on the FUSER system file from within the library. If the option is set to "Y", users need at least ALTER access to make modifications on the FUSER file.

## Translation and Effects of Access Levels

The following table shows how CA-ACF2 translates RACF attributes, and also gives an overview of the effects of the access levels:

RACF Attribute	CA-ACF2 Resource Rule	Disabling of Natural Commands	Read-Only FUSER System File
READ	READ	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
UPDATE	UPDATE	Commands are disabled (same as profile parameter NC=ON).	FUSER file is read-only.
CONTROL	DELETE	Commands are allowed (same as profile parameter NC=OFF).	FUSER file is read-only.
ALTER	ADD	Commands are allowed (same as profile parameter NC=OFF).	Modification on FUSER file are allowed.

## RPC Services

With Natural SAF Security, Natural RPC services can be protected against unauthorized use.

You can protect a Natural RPC service:

- independently of the environment, or
- in specific environments.

The resource-class name for Natural RPC services is defined with the macro parameter NACL SV in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NSVSAG".

## Environment-Independent Use of an RPC Service

If a Natural RPC service is to be protected, a resource profile has to be defined for it in the external security system.

The resource-profile name must correspond to the library ID and subprogram name, each of which may be up to 8 characters long and which must be separated by a period:

*library-ID.subprogram-name*

The option "Protect Services" in the General NSF Options determines if access to Natural RPC services is to be controlled by Natural SAF Security. If this option is set to "Y", the access level defined for the RPC service in the external security system determines whether a user can use the service or not. A user needs at least READ access to be able to execute a Natural subprogram via RPC.

## Use of an RPC Service in Specific Environments

If a Natural RPC service is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-service combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name must consist of the alias, the library ID (up to 8 characters), and the subprogram name, separated from one another by periods:

*a.library-ID.subprogram-name*

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific service-access check is activated by the option "with Environment" in the RPC Options section of the General NSF Options. Use of the RPC service is then only possible in environments to which the user has READ access.

## User-Defined Resources

With Natural SAF Security, user-defined resources can be protected against unauthorized use.

You can protect a user-defined resource:

- independently of the environment, or
- in specific environments.

The resource-class name for user-defined resources is defined with the macro parameter NACLAP in the configuration module of the SAF server (see Step 4 of the Natural SAF Security installation procedure). The default name is "NPGSAG".

## Environment-Independent Use of a User-Defined Resource

If a user-defined resource is to be protected, a resource profile has to be defined for it in the external security system.

The name of a resource profile can, for example, consist of a library ID, main function and subfunction. The library ID may be up to 8 characters long, the main function is usually (but not necessarily) the name of the programming object, and the subfunction is a 3-character code identifying the function to be performed. Each of the three must be separated from one another by a period:

*library-ID.main-function.sub-function*

The resource profile determines whether a user may access a user-defined resource or not.

The necessary security requests are handled via user exits provided by Natural SAF Security. The user exits are described in the section User Exits.

## Use of a User-Defined Resource in Specific Environments

If a user-defined resource is to be protected in a specific Natural environment (Natural system-file combination), a resource profile has to be defined for the environment-resource combination in the external security system. A Natural environment is determined by a one-character alias. The resource-profile name is composed as above, prefixed by the alias, for example:

*a.library-ID.main-function.sub-function*

In Natural SAF Security, you have to define an environment profile for the environment. In the environment profile, the alias to be used has to be specified.

The environment-specific resource-access check is activated by the option "with Environment" in the User-Resource Options section of the General NSF Options.

The necessary security requests are handled via user exits provided by Natural SAF Security. The user exits are described in the section User Exits.

## Overview of Resource-Class Definitions

The following table summarized the resource-class definitions to be made in the configuration module of the SAF server:

<b>Resource</b>	<b>Macro Parameter in Configuration Module</b>	<b>Default Name</b>	<b>Length of Resource-Profile Name</b>
Environments	NACLSF	NSFSAG	40
Libraries	NACLTC	NTCSAG	10
RPC services	NACLSV	NSVSAG	19
User-defined resources	NACLAP	NPGSAG	23