Introducing Natural SAF Security

This section provides an overview of Natural SAF Security. It covers the following topics:

- What is Natural SAF Security?
- Configuring Your Security Environment - an Example
- Natural Security Related Considerations
- Natural SAF Security in Batch Mode

What is Natural SAF Security?

Natural SAF Security (NSF) is an add-on product to Natural Security. It allows you to control users' access to Natural based on user and resource definitions made in an external security system. With Natural SAF Security, you can thus protect your Natural sessions by combining security definitions made in Natural Security and security definitions made in the external security system.

This external security system must be an SAF-compliant security system. At present, Natural SAF Security supports the following external security systems:

- RACF,
- CA-ACF2,
- CA Top Secret.

When you use Natural SAF Security, you need not define users both in Natural Security and in an external security system; it is sufficient to define them in the external security system. In Natural Security, only user *groups* are defined. When Natural SAF Security is active and a user logs on to Natural, the user authorization checks will be done using the user ID and user password from the external security system. After the authorization, further security checks - particularly concerning the use of Natural libraries and utilities - will be based on the user *group* definitions in Natural Security. Although library protection via an external security system is possible, the Natural Security library security profiles provide more sophisticated and more adequate mechanisms for protecting Natural libraries.

In addition, access to Natural can be made environment-specific. A Natural environment is determined by the combination of the system files FNAT, FUSER, FDIC and FSEC. Natural environments can be defined in the external security system. By defining environments and controlling their accessibility, it is possible, for example, to fully separate the protection of a Natural development environment from that of a Natural production environment. At the same time, this avoids system-file mix-ups (for example, a test-environment FSEC file in conjunction with a production-environment FUSER file).

Also, instead of the end of transaction IDs (ETIDs) from Natural Security user profiles, Natural SAF Security provides various possibilities of generating unique ETIDs.

Moreover, Natural SAF Security allows you to protect user-defined resources which are defined in the external security system against unauthorized use.

Configuring Your Security Environment - an Example

This section is an example of the usage of Natural SAF Security. It does not cover all aspects or possibilities offered by Natural SAF Security. In particular, it does not cover all Natural SAF Security options (NSF options). Instead, a few selected options are introduced to show you how you can set up your security environment step by step:

- user security,
- environment security,
- environment-specific library security.

Although the following explanations are based on certain assumptions, some of which may not apply to your security environment, this approach may be helpful to make yourself familiar with Natural SAF Security.

If you are not yet familiar with Natural SAF Security, it is recommended that you deal with the NSF options step by step as indicated in the explanations below, and only change those options mentioned below.

Generally, please bear in mind that before you set any NSF options, you have to make sure that the corresponding resources are defined in the external security system being used. For resource definitions, see the section *Defining Resources in the External Security System and Activating Them*.

User Security

The desired security setup is assumed to be as follows:

- User security data are to be maintained not in both Natural Security and your external security system, but primarily in the external security system.
- For the logon on to Natural, the user security data (user ID and password) as defined in the external system are to be used, and the user authentication is to be performed by the external security system according to the authentication rules defined in the external security system.
- Apart from the user authentication, the logon to Natural is to be performed by Natural Security according to the Natural Security logon rules.
- *Within* the Natural session, Natural Security controls what the user is allowed to do.

The necessary connection between the external security system and Natural Security is made by using user *groups* in both systems.

The above setup requires that:

- users and user groups are defined in the external security system,
- the user groups are also defined in Natural Security,
- a connection between the group definitions in the external security system and the group definitions in Natural Security is established.

Except for users with special tasks (for example, Natural Security administrators), you need not create security profiles for individual users in Natural Security, nor assign them to groups; it is sufficient that users are defined and assigned to groups in the external security system.

To establish the desired setup, you have to do the following:

In the external security system:

- Make sure that users and user groups are defined appropriately.

In Natural Security:

- Create a group security profile for every user group which is defined in the external security system. As ID for the security profile use the same ID by which the group is defined in the external security system. It is recommended that you specify a default library in the group security profile.
- In "Administrator Services > General Options > User Options" (third screen of General Options), set the following options:
  - Set "NSF *GROUP" to "Y".
  - Set "NSC Group ID" to "Y".

Environment Security

A Natural environment is determined by the combination of the system files FNAT, FUSER, FDIC and FSEC. When a users accesses a library, these are determined by the current values of the corresponding Natural profile parameters - with the following exception: If the Natural Security library profile of that library contains another FUSER value, this will overwrite the FUSER profile parameter.

Based on the user-security setup as described above, the desired security setup for Natural environments is assumed to be as follows:

- Access to Natural environments is to be controlled, so that not all users have access to all environments.

This setup requires that Natural environments are defined in the external security system. Access authorization to the environments will then be controlled according to the access rules defined in the external security system.

To establish the desired setup, you have to do the following:

- In the external security system: Define resource profiles for all Natural environments (system-file combinations) to be protected.
- In Natural Security: In "Administrator Services > General Options > Environment Options (fourth screen of General Options), set the option "Protect Environments" to "Y".

Environment-Specific Library Security

Based on the user-security setup described above, the desired security setup for environment-specific library protection is assumed to be as follows:

- Library security data continue to be maintained in Natural Security.
- Access to Natural libraries is to be controlled by Natural Security, that is, access to libraries will be according to the Natural Security logon rules.
- In addition, access to a library is to be restricted to certain Natural environments (as determined by the combination of the system files FNAT, FUSER, FSEC and FDIC); for example, some users are to access a library only in a development environment, others only in a production environment.

The necessary connection between the external security system and Natural Security is made via one-character aliases. The environment-specific access authorization to a library is checked as follows: When a user attempts to access a library, the environment in which the library is located is determined by the current values of the Natural profile parameters FNAT, FDIC, FSEC and FUSER - with the FUSER value being overwritten by the one specified in the Natural Security library profile. For this environment, a Natural Security environment profile has to exist, in which a one-character alias is specified. For the combination of this alias and the library (*alias.library-ID*), a resource profile has to exist in the external security system. The access level defined in this resource profile determines whether the user is allowed to log on to the library in that environment.

To establish the desired setup, you have to do the following:

In the external security system:

- Make sure that the resource profiles for the Natural libraries are defined with the same IDs by which the libraries are defined in Natural Security.
- Define a resource profile for every environment-library combination (that is, *alias.library-ID*) to be protected.

In Natural Security:

- Define an environment profile for every Natural environment (system-file combination).
- In "Administrator Services > General Options > Library Options (fourth screen of General Options), set the following options:
  - Set "Protect Libraries" to "Y".
  - Set "with Environment" to "Y".

Natural Security Related Considerations

The following Natural Security items should be considered when using Natural SAF Security.

Library SYSSEC

The library SYSSEC can only be accessed by users who, in addition to being defined in the external security system, are defined as "Administrators" in Natural Security.

Automatic Logon

If the Natural profile parameter AUTO=ON (Automatic Logon) is set, a user can only log on to Natural if a default library is defined for him/her. The default library can be specified in the Natural Security group security profile. See also the section *Automatic Logon* in the *Natural Security* documentation.

Natural SAF Security provides a user option "NSC Logon Priv. Library" by which it is possible that a user who logs on without specifying a library ID will be logged on to the library whose ID is the same as the current value of the Natural system variable *USER value.

PROFILE Command

When Natural SAF Security is active, the Natural system command PROFILE indicates whether the user and his/her group are defined in Natural Security:

- If neither the current user ID nor group ID are defined in Natural Security, the user type will be shown as "Ext. User".
- If the current user ID is not defined in Natural Security, but the current group ID is defined in Natural Security, the user type will be shown as "Ext. User/Grp".

Transition Period Logon

If the Natural Security general option Transition Period Logon is set to "N", only unprotected libraries can be accessed via Natural SAF Security. Undefined libraries can only be accessed if Transition Period Logon is set to "Y".

Utilities

For users for whom neither a user security profile nor a group security profile exists in Natural Security, the default utility profiles apply.

For users for whom no user security profile, but a group security profile exists, the use of utilities is controlled by the group-library-specific utility profiles and group-specific utility profiles associated with this group.

Natural SAF Security provides an additional utility: SAF Online Services (SYSSAFOS). To be able to access this utility, a utility security profile for SYSSAFOS has to be defined in Natural Security.

Utility profiles are described in the section *Protecting Utilities* of the *Natural Security* documentation.

Natural SAF Security in Batch Mode

For information on logging on to Natural SAF Security in batch mode, see the section *Natural Security In Batch Mode* in the *Natural Security* documentation. What is said there also applies to Natural SAF Security. However, please bear in mind that for the logon, the user ID and password as defined in the external security system are used, and have to comply with the authentication rules defined in the external security system.