Installing and Activating Natural SAF Security

This section describes how to install and activate Natural SAF Security under z/OS systems using an Adabas database.

- Installation Prerequisites
- Installation Tape - z/OS
- Installation Procedure
- Activation

Notation vrs or vr: If used in the following document, the notation *vrs* or *vr* stands for the relevant **v**ersion, **r**elease, **s**ystem maintenance level numbers. For further information on product versions, see Version in the *Glossary*.

Installation Prerequisites

Natural SAF Security can only be installed if supported versions of the following products have been installed (for information on supported version, see the section *Natural and Other Software AG Products* in the current Natural *Release Notes*):

- Natural,
- Natural Security,
- Adabas,
- Adabas Limited Libraries,
- an SAF-compliant security system.

Installation Tape - z/OS

The installation tape contains the datasets listed in the table below. The sequence of the datasets is shown in the *Report of Tape Creation* which accompanies the installation tape.

Dataset	Contents
NSF*vrs*.INPL	Natural INPL dataset containing updates to Natural SAF Security.
NSF*vrs*.LOAD	Load library containing the Natural SAF Security assembly module NATGWSAF.

Installation Procedure

This section describes step by step how to install Natural SAF Security.

Step 1: Load Modules

(Job I005)

Load the Natural SAF Security modules using the Natural utility INPL (assigning dataset NSF*vrs*.INPL to work file CMWKF01).

Step 2: Adjust Natural Parameter Module

(Job I010)

Add the following parameter to your Natural parameter modules:

```
DS=(NSFSIZE,8)
```

Or, using the NTDS parameter macro:

```
NTDS NSFSIZE,8
```

8 KB is the minimum NSFSIZE value. Depending on your usage of Natural SAF Security, a higher value may be required, which can be calculated as follows:

4 KB + (*e* * 17 bytes) + ((*p* + *r*) * 8 bytes), rounded up to the next KB

where:
e is the number of protected environments,
p is the number of protected programming objects,
r is the number of protected RPC services.

If you wish to use Natural SAF Security to control the execution of Natural programming objects, you also have to add the following parameters to your Natural parameter modules:

```
RDCEXIT=(RDCEX3,2000)
RDCSIZE=2
```

Note:
If this feature is used, you have to either link the Natural SAF Security assembly module NATGWSAF to the Natural parameter modules or to the Natural nucleus (in the case of a shared nucleus, to the environment-independent part).

Then reassemble the parameter modules.

Step 3: Relink Natural

(Job I060 from the Natural installation tape)

Relink your Natural nucleus to include the modified parameter module and Natural SAF Security modules:

```
INCLUDE SMALOAD(NATPARM)
INCLUDE NSFLOAD(NATGWSAF)
```

Step 4: Install the SAF Server

The SAF server (SAF Security Kernel) is delivered with Adabas Limited Libraries.

Install and configure the SAF server and its associated Daemon as described in the *SAF Security Kernel* documentation.

In the configuration module of the SAF server, the following Natural SAF Security options may have to be set:

Number of Cached Resource Checks

Natural SAF Security allows you to have resource checks cached. If you wish resource checks to be cached, you have to specify the number of successful resource checks to be cached for each resource class, using the following parameters of the configuration module:

Parameter	Default Value	Function
NANUSF	0	Number of cached environment checks.
NANUTC	0	Number of cached library checks.
NANURP	0	Number of cached RPC-service checks.

Alternate Resource Names

If you wish to change the default names for the resource classes, you have to change the following parameters of the configuration module:

Parameter	Default Value	Function
NACLSF	SAGNSF	Resource-class name for environments.
NACLTC	SAGNTC	Resource-class name for libraries.
NACLPG	SAGNPG	Resource-class name for programming objects.
NACLRP	SAGNRP	Resource-class name for RPC services.
NACLAP	SAGNPG	Resource-class name for user-defined resources.

After the above steps have been performed, the installation of Natural SAF Security is complete.

To be able to use Natural SAF Security, you have to activate it as described in the following section.

Activation

The activation of Natural SAF Security comprises the following steps:

1. Activate Natural SAF Security Itself

2. Define SYSSAFOS Utility Profile
3. Start SAF Server
4. Check Connections and Data Transfer

Activate Natural SAF Security Itself

Before you activate Natural SAF Security, you should define the necessary resources in the external security system, as described in the section *Defining Resources in the External Security System and Activating Them*. In particular, do not set any Natural SAF Security options other than the ones mentioned below, unless you have defined the corresponding resources in the external security system.

If you are not yet familiar with Natural SAF Security, it is recommended that you read the section *Introducing Natural SAF Security* before you activate it.

The activation of Natural SAF Security has to be performed within Natural Security. You have to meet the following prerequisites to be able to activate Natural SAF Security:

- You must be defined as a user of type "Administrator" in Natural Security.
- You must be linked to the library SYSSEC in Natural Security.

To activate Natural SAF Security:

1. Invoke Natural and log on to the Natural Security library SYSSEC.
2. On the Natural Security Main Menu, select "Administrator Services". The Administrator Services Menu will be displayed.
3. Select "General options". The Set General Options screen will be displayed.
4. Press PF8 twice. The General Options 3 (NSF) screen will be displayed.
5. On this screen:
   - Set all four options listed under "Security System": Specify values for the fields "External Security System", "Server ID" and "Natural Security", and set the field "Protection Level" to "2". For details on these fields, see *NSF Options*. The setting of these four options activates Natural SAF Security.
   - Set the option "NSF *USER-NAME", which is listed under "User Options", to "Y". This will be used by the check described below.
   - *Do not* change the values of any other fields on the screens General Options 3 (NSF) and General Options 4 (NSF)!
6. For the activation of Natural SAF Security to take effect, end your Natural session.

The activation as described above only "switches on" Natural SAF Security as such, using default settings. The subsequent configuration of your security environment can then be performed gradually step by step as outlined in the section *Introducing Natural SAF Security*.

Define SYSSAFOS Utility Profile

The utility library SYSSAFOS, which was loaded by the Natural SAF Security installation procedure, contains the SAF Online Services. To be able to access this utility, you have to define a utility security profile for SYSSAFOS in Natural Security (as described in the section *Protecting Utilities* of the *Natural Security* documentation).

Start SAF Server

Once Natural SAF Security has been activated, start the SAF server, as described in the *SAF Security Kernel* documentation.

If the SAF server is already running (which may be the case if it is being used by another product), restart it.

Access to Natural is now controlled by Natural SAF Security.

Check Connections and Data Transfer

Log on to Natural (with Natural profile parameter AUTO=OFF), using the password which is defined for you in the external security system.

Within your Natural session, enter the system command PROFILE.

If the logon with that password has been successful, and the field User Name on the PROFILE screen shows the name by which you are defined in the external security system, this confirms that the connections between the external security system, the SAF server and Natural SAF Security are established, and that the data transfer from the external security system to Natural SAF Security works correctly.