Add-On Products and Plug-Ins

This section contains information on the protection of various Natural add-on products by Natural Security and the handling of plug-ins in a Natural Security environment. It contains information on:

- Plug-Ins under Natural Security
- SYSDIC under Natural Security
- SYSAOS under Natural Security

Plug-Ins under Natural Security

The Natural Studio user interface is extensible by plug-ins. If plug-ins are used in an environment protected by Natural Security, the following prerequisites must be met:

Library Profiles for System Libraries

For the Natural Plug-in Manager (which is a plug-in itself) and for every plug-in to be used, a library security profile has to be defined. For plug-ins delivered together with Natural Studio, pre-defined system-library profiles are provided. To activate these, you use the Administrator Services function "Definition of system libraries".

The following plug-in system libraries are provided:

Library	Contents
SYSEXPLG	Plug-in Example.
SYSPLCGC	Program Generation.
SYSPLMAN	Plug-in Manager.
SYSPLMFE	Mainframe Navigation.
SYSPLNEE	Metrics Calculation / Engineer Xref Viewing.
SYSPLPDC	Object Description.
SYSPLPGC	Schema Generation.
SYSPLWEB	Web Interface.
SYSPLWIZ	Application Wizard.
SYSPLXRC	Xref Evaluation.

User Profiles

When a user activates a plug-in, Natural Studio starts a second Natural session with automatic logon (profile parameter AUTO=ON). For the automatic logon to be successful, a user who is to use a plug-in must have either a default library or a private library specified in his/her security profile.

Natural Parameter File

When a user activates a plug-in, Natural Studio starts a second Natural session using the parameter file NATPARM. If the user's Natural session uses a parameter file other than NATPARM, the system-file specifications for FNAT, FSEC and FUSER in the NATPARM parameter file must match those of the parameter file used by the user session in a Natural Security environment.

SYSDIC under Natural Security

On mainframe computers, the Predict library SYSDIC may be defined and its use controlled by Natural Security.

Library Profile for SYSDIC

To be able to use under Natural Security those Predict functions which use Adabas Online Services (AOS) facilities, that is, to enable Natural Security protection, you have to perform the following steps:

1. Create a security profile for the library SYSDIC (Add Library).
2. Define the library SYSDIC as people-protected, and link to it those users (or user groups) who are to be Predict/AOS administrators.
3. Execute the program NSCPRDAX in the library SYSSEC. This program writes the user exit NSCPRD01 into the SYSDIC library profile.
4. Invoke the Modify Library function for the library SYSDIC. Even if you do not change anything in the security profile, you must perform this step to confirm the entry of the user exit, because otherwise Natural Security would consider the execution of NSCPRDAX an illegal manipulation of SYSDIC's security profile, and no-one would be able to log on to SYSDIC.

After the user exit has been written into the security profile, no Predict functions will be available until Predict security profiles are defined.

The user exit cannot be removed manually from the SYSDIC library profile. To remove it, you execute the program NSCPRDDX in the library SYSSEC, and then invoke the Modify Library function for confirmation (as with Step 4 above).

Database Security Administrators

When you select "User Exit" from the Additional Options of SYSDIC's library profile, an additional screen "Predict/AOS Security Profile" is displayed. On this screen, you specify who is to be AOS security administrator for which database. The users (or groups of users) specified may then use the AOS-related Predict functions for these databases.

For each database, you can only specify one AOS security administrator. This may be a user of type ADMINISTRATOR, PERSON, MEMBER, or a GROUP (it need not be a Natural Security administrator). The user must be linked to the library SYSDIC before he/she can be specified as AOS security administrator.

Further Information

For further information on Predict and its AOS-related functions, and on Predict under Natural Security, please refer to the Predict documentation.

SYSAOS under Natural Security

On mainframe computers, the Adabas Online Services library SYSAOS may be defined and its use controlled by Natural Security.

Library Profile for SYSAOS

To be able to use the Security Maintenance section of Adabas Online Services under Natural Security, that is, to enable Natural Security protection for Adabas Online Services, you have to perform the following steps:

1. Create a security profile for the library SYSAOS (Add Library).
2. Define the library SYSAOS as people-protected, and link to it those users (or user groups) who are to be Adabas Online Services database administrators.
3. Execute the program NSCAOSIX in the library SYSSEC. This program writes the user exit NSCAOSE1 into the SYSAOS library profile.
4. Invoke the Modify Library function for the library SYSAOS. Even if you do not change anything in the security profile, this step is necessary to confirm the entry of the user exit, because otherwise Natural Security would consider the execution of NSCAOSIX an illegal manipulation of SYSAOS’s security profile, and no-one would be able to log on to SYSAOS.

After the user exit has been written into the security profile, no Adabas Online Services functions will be available until Adabas Online Services security profiles are defined.

The user exit cannot be removed manually from the SYSAOS library profile. To remove it, you execute the program NSCAOSDX in the library SYSSEC, and then invoke the Modify Library function for confirmation (as with Step 4 above).

Note:
Previous versions of Natural Security supplied the user exit NSCAOS01, which can still be used instead of NSCAOSE1. With NSCAOS01, however, a maximum of only 72 database profiles can be maintained with Adabas Online Services, while up to 156 can be maintained with NSCAOSE1. Unlike NSCAOSE1, NSCAOS01 does not allow you to assign more than one user group as an administrator to the default database (see below). The program used to write NSCAOS01 into the library profile of SYSAOS is called NSXAOSAX. Otherwise, what is said above about NSCAOSE1 also applies to NSCAOS01.

Database Security Administrators

When you select "User Exit" from the Additional Options of SYSAOS’s library profile, an additional screen "Adabas Online Services Security Profile" is displayed. On this screen, you specify who is to be Adabas Online Services security administrator for which database. The users (or groups of users) specified may then use the Security Maintenance section of Adabas Online Services for these databases.

For each database, you can only specify one Adabas Online Services security administrator. This may be a user of type ADMINISTRATOR, PERSON, MEMBER, or a GROUP (it need not be a Natural Security administrator). The user must be linked to the library SYSAOS before he/she can be specified as Adabas Online Services security administrator.

Adabas Online Services uses the database profile for database ID 999 as a default profile, which applies to all databases for which no individual database profiles are defined. With the user exit NSCAOSE1, you can assign more than one group of Adabas Online Services security administrators to database 999. To do so, you specify "********" (8 asterisks) as the administrator ID for database 999 in the SYSAOS library profile. The administrators for database 999 are then determined by the database profile in Adabas Online Services. As Adabas Online Services allows you to define more than one profile per database, you can define multiple profiles for database 999, each with a different group of administrators.

Further Information

For further information on Adabas Online Services, please refer to the Adabas documentation.