

General Information for Natural Security

This section covers the following topics:

- General Installation Information
- Natural Security in a Heterogeneous Environment

Platform-specific installation procedures:

- Installing Natural Security under OpenVMS
 - Installing Natural Security under UNIX
-

General Installation Information

It is recommended that you install Natural Security *after* having installed all other subproducts of Natural, as this makes defining the subproducts' system libraries to Natural Security easier.

Once Natural Security is installed, Natural on the assigned system file (FNAT) can only be accessed under the control of Natural Security. Natural Security cannot be removed once it has been installed. It is therefore recommended that you make a backup copy of your FNAT system file before you install Natural Security.

Shared Natural Security System File FSEC

As of Natural Security Version 2.2, it is no longer necessary to create a new Natural Security system file (FSEC) for a new Natural Security version. This means that you do not need separate FSEC files for different Natural Security versions.

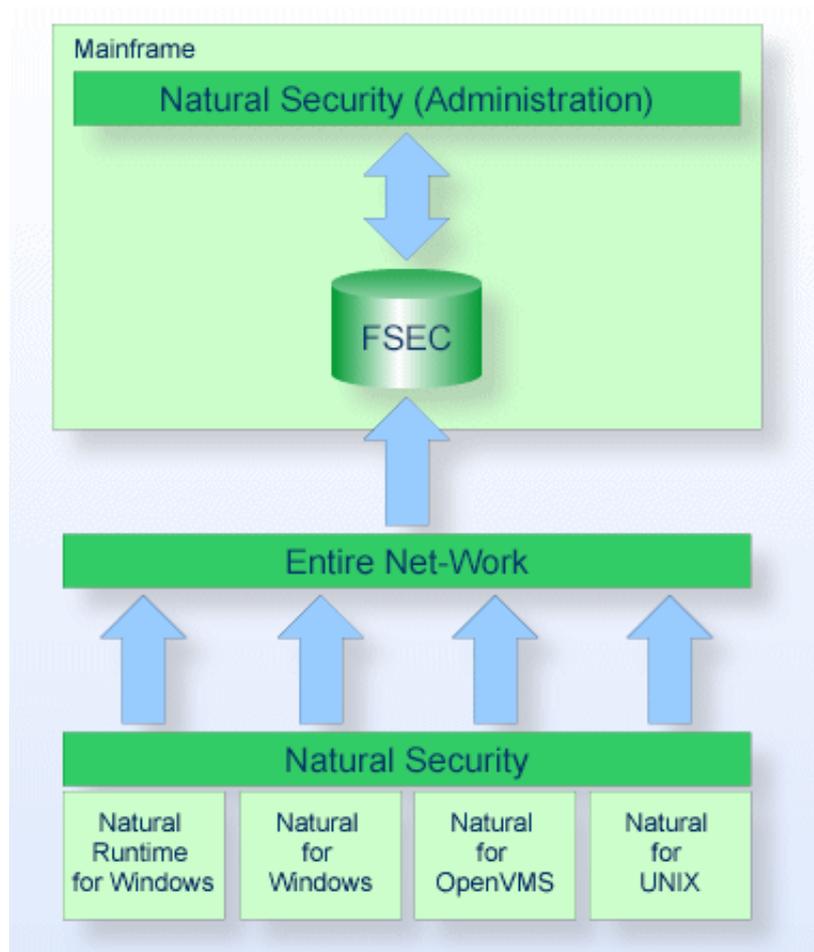
Instead you can keep an existing (Version 2.2 or above) FSEC file and share it between different Natural Security versions. This also means that you do not have to transfer your existing Natural Security data to another FSEC file or convert them.

If you use an FSEC file shared by different Natural Security versions, always use the highest of these versions for the maintenance of your Natural Security data in order to ensure the consistency of your data.

Natural Security in a Heterogeneous Environment

With Natural Security for mainframes, all enterprise security profile data can be stored and administered centrally in a mainframe system file, which is accessible to a heterogeneous environment, thus simplifying and standardizing security maintenance on a company-wide basis. The security data in the mainframe Natural Security system file (FSEC) can be retrieved via remote database calls, managed by Entire Net-Work, from the following Natural Security installations:

- Natural Runtime for Windows
- Natural for OpenVMS
- Natural for UNIX
- Natural for Windows



From the non-mainframe Natural Security installations, you can log on to the Natural Security mainframe environment and retrieve security data.

However, in the non-mainframe Natural Security installations, the security data maintenance application SYSSEC is disabled, as are the following Natural Security interface subprograms for modifying security profiles:

- NSCLI
- NSCOB
- NSCMA
- NSCUS

If these interface subprograms are invoked, Error NAT0828 is returned.

For further information on setting up Natural Security in a heterogeneous environment, see below.

Setting Up Natural Security in a Heterogeneous Environment

Configuring Entire Net-Work

Entire Net-Work's translation process is based upon the format and length of each field specified in the search and format buffers that are passed with each Adabas call, along with special translation definition parameters. When a request goes through the network conversion routines, each individual field is translated according to the format and length defined for it in the associated search or format buffer.

To avoid the errors NAT0824 and NAT0825, add translation definitions for the following fields for the DBID and FNR of the mainframe system file FSEC with format "X":

- LW
- LC
- LQ
- LV
- LS

This prevents values being either translated or swapped.

For further information, see the section **Special Handling of Field Format "X"** in the section **Heterogeneous Platform Considerations** in the Entire Net-Work Installation and Operations for Mainframes documentation.

Customizing the Natural I/O Conversion Table on Non-Mainframe Platforms

If you want to use special characters not contained in the default Natural character set (ISO08859), for example in passwords, you must customize the Natural I/O conversion table in the following sections of the file NATCONV.INI:

ISO8859_1->EBCDIC

EBCDIC->ISO8859_1

You can use the call CMCNV provided in the module SULCONV in the library SYSTRANS to check the settings.

For further information on the file NATCONV.INI, see your Natural Operations documentation.

Setting Up Module Access

When you are using Natural Security across platforms, security profiles held in the mainframe FSEC system file will usually apply to data held in libraries on another platform.

If you use the Allow/Disallow Modules definition, it is recommended that you use the "Module names held in the user buffer" fields of the library maintenance function Disallow/Allow Modules screen. For modules which are not on the mainframe FUSER, use the Free List.

For further information, see the section on disallowing/allowing modules in the Natural Security for Mainframes documentation.

Setting Up Natural DDM Security

If you want to use a non-mainframe platform as your Natural development environment, you must move any DDMs required by Natural modules to the library SYSTEM (FUSER). This is necessary because Natural Security runtime only checks DDMs located in the library SYSTEM.