Natural Security On Different Platforms

This section covers the following topics:

- Supported Platforms
- Using Natural Security on Multiple Platforms

Supported Platforms

Natural Security is available on the following platforms:

- mainframe computers,
- UNIX,
- OpenVMS,
- Windows.

Natural Security is available as a full version and as a runtime version.

Full Version

Normally, Natural Security is installed as a full version comprising the complete functionality of Natural Security. The full version can be installed on all platforms - except on some Windows platforms (as listed in the Natural *Release Notes*), where only the runtime version is available.

The full version comprises the entire runtime functionality as well as the full administrative and maintenance functionality. In the application SYSSEC it provides all functions for the online administration and maintenance of Natural Security data, and for the creation and evaluation of access logs, as well as application programming interfaces for the retrieval and maintenance of Natural Security data.

Runtime Version

On those Windows platforms which are not suited to the stand-alone operation of Natural, Natural Security is installed as a runtime-only version, which only contains the functionality necessary to enable user authentication and access control of Natural resources: it includes the logon procedure, which performs user authentication and verification of access rights when a user logs on to a Natural session, plus the procedures which perform access control to check whether a user has permission to perform the desired functions within a Natural session. In addition, retrieval functions provided by the Natural Security application programming interfaces are available.

As the runtime version does not include any maintenance capability, it requires access to a Natural Security system file (FSEC) on another platform. Thus, a runtime version can only be used in combination with a full version installed on one of the other platforms.

Using Natural Security on Multiple Platforms

This section covers the following topics:

- Central FSEC System File
- Protection of Programming Objects
- Protection of DDMs
- Character Translation in Client/Server Environments
- Configuring Entire Net-Work

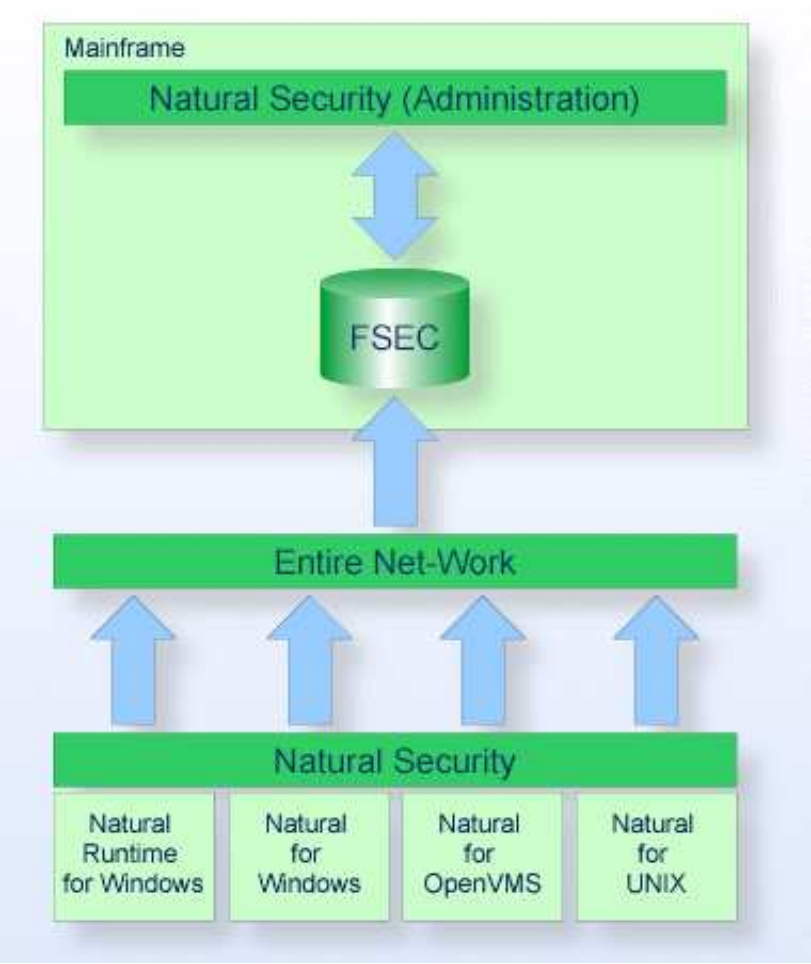
Central FSEC System File

In a heterogeneous, multiple-platform Natural environment, the administration and retrieval of Natural Security data has to be taken into consideration. It is possible to set up a separate Natural Security system file (FSEC) for each installation, and maintain each FSEC system file independently.

It is also possible to set up a single FSEC system file in which all Natural Security data are stored centrally. The Natural Security installations have to be connected in a network with Entire Net-Work. Access to the centrally stored security data is handled by Entire Net-Work by means of remote database calls.

If the multiple-platform configuration does not include a mainframe, the FSEC system file can be located and the Natural Security data maintained on any of the (full version) installations; however, it is recommended that you maintain them on the installation where the FSEC system file is local.

If the multiple-platform configuration includes a mainframe, the FSEC system file must be located and the Natural Security data maintained on the mainframe. On the non-mainframe installations, the maintenance of Natural Security data is then automatically disabled. This includes maintenance via Natural Security’s application programming interfaces.



The accessibility of an FSEC system file in a multiple-platform configuration is as follows:

Location of FSEC	Accessible from
Mainframe	Mainframe, UNIX, OpenVMS and Windows
UNIX	UNIX, OpenVMS and Windows
OpenVMS	OpenVMS, UNIX and Windows
Windows	Windows, UNIX and OpenVMS

In a heterogeneous environment, the following has to be considered concerning the protection of programming objects and DDMs:

Protection of Programming Objects

In a heterogeneous production environment using a central mainframe FUSER system file, a library which does not exist on the mainframe FUSER system file but in the file system on another platform would not be known to Natural Security on the mainframe. To be able to define "non-existent" modules contained in such a library, the Disallow/Allow Modules function provides the subfunction "Free List of Modules" (which is described in the section *Library Maintenance*).

With the option Module Protection Mode (described in the section *Administrator Services*), it is possible to make Natural Security's protection of programming objects uniform across all mainframe and non-mainframe platforms.

Protection of DDMs

Natural's storage location for DDMs is not the same on all platforms: on mainframe computers, DDMs are stored in an FDIC system file, whereas on UNIX, OpenVMS and Windows, DDMs are contained in libraries like other Natural objects. Therefore, Natural Security's handling of the DDM protection is also different:

- On mainframe computers, DDMs are treated as separate objects (called "files"), which have their own security profiles.
- On the non-mainframe platforms, the protection of DDMs is subordinate to the protection of libraries, and DDM security profiles are subordinate to library security profiles.

For further information, see *DDM/Files* in the section *Structure And Terminology Of Natural Security*.

In a heterogeneous environment where a central FSEC system file on a mainframe is used, all DDMs on the non-mainframe platforms must be transferred to the library SYSTEM in order to enable their use under Natural Security.

FDDM Profile Parameter

If a system file as the central location for DDM storage (outside of libraries) is specified with the Natural profile parameter FDDM on a non-mainframe platform, the protection of non-mainframe DDMs and the maintenance of their security profiles is performed in the same way as with mainframe DDMs.

Character Translation in Client/Server Environments

If Natural Security is used on multiple platforms in a client/server environment, and a logon is performed on a client which uses a different character code than the server, Natural Security has to translate the logon data from ASCII to EBCDIC or vice versa on the server. For this character translation, Natural Security uses the following translation tables:

- On mainframes, it uses the translation table NTTABA2 in the Natural configuration module NATCONFG.
- On non-mainframe platforms, it uses the sections "ISO8859_1->EBCDIC" and "EBCDIC->ISO8859_1" of the Natural configuration file NATCONV.INI.

If these do not suit your requirements, you may have to adjust them. For further information, see the Natural *Operations* documentation for the relevant platform.

Configuring Entire Net-Work

Entire Net-Work's translation process is centered around 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 FSEC system file with format "X":

- LW
- LC
- LQ
- LV
- LS

This prevents values from being either translated or swapped.

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