Protecting the Natural for Eclipse Environment

This section describes how to control the use of the server and navigator views used by Natural for Eclipse. It covers the following topics:

- Protecting the Natural Server View for Eclipse

- Protecting the Eclipse Navigator View

Protecting the Natural Server View for Eclipse

This section describes how to protect with Natural Security a Natural server used in Eclipse, and how the security definitions on the FSEC system file attached to the server environment affect actions on the server. It covers the following topics:

- Map Environment and Library Selection

- Protectable Functions in the Mapped Environment

Map Environment and Library Selection

The function "Map Environment" is controlled by the Natural Security settings that apply to the FNAT system file on which this function is executed. When the function is executed, Natural Security performs a logon, according to the rules as described in the section *Logon Procedure*. The logon will be to the user's default library, therefore the security settings have to be such that the user is able to log on to his/her default library.

Once the environment has been mapped, the server view in the mapped environment lists all non-empty libraries on the FUSER system file assigned to the mapped environment which are accessible by the user. Libraries in whose security profiles a different Library File is specified are not listed.

When the user selects one of these libraries from the server view, a logon to this library is performed - according to the rules as described in the section *Logon Procedure*. Thus it may be possible, for example, that a startup transaction is executed. The user can only select a library from the tree view; any other library selection (for example, via the system command "LOGON *") is not possible.

Within a library in the mapped environment, some functions can be protected by Natural Security, others cannot be protected. Which functions these are is described below.

The Natural Security data used by the Natural Server view are cached and will only be refreshed when the Natural server is mapped again.

Note:
If a startup transaction is defined for any library in the Natural Server view, it will not be executed (and the Natural system variable *STARTUP will not be set).

Protectable Functions in the Mapped Environment

The use of the following functions in a library within the mapped environment can be protected as follows:

- Server-View Actions

Disallowed actions are disabled in the context menus of the Natural Server view.

Server-View Actions

Note:
Several of the server-view actions listed below are controlled by SYSMAIN utility profiles. If, however, no utility profiles for SYSMAIN are defined, these actions are controlled by the Utilities option in the library profile of the library processed.

Location in Server View	Action	Controlled by
System-file node	Unlock	Session Option "Unlock Objects" in user security profile.
Library node	Open / Add to New Project / Add to Existing Project	Command Restrictions (LIST or READ command) in library security profile*.
	Rename **	The action as such is always allowed and cannot be disallowed. However, a library security profile for the library of the new name must exist (unless the general option Transition Period Logon is set to "Y"). Also, for the library contents to be transferred, the option "Mo" (Move) "from library" and "to library" for all object types must be allowed in the SYSMAIN utility profile.
	Delete **	Option "De" (Delete) for object type in SYSMAIN utility profile.
	Copy	Option "Co" (Copy) "from library" for object type in SYSMAIN utility profile.
	Paste	Option "Co" (Copy) or "Mo" (Move) "from library" for object type in SYSMAIN utility profile.

Location in Server View	Action	Controlled by
Group node	Open / Add to New Project / Add to Existing Project	Command Restrictions (LIST or READ command) in library security profile*.
	Delete	Command Restrictions in library security profile*.
	Copy	Option "Co" (Copy) "from library" for object type in SYSMAIN utility profile.
	Paste	Option "Co" (Copy) or "Mo" (Move) "from library" for object type in SYSMAIN utility profile.
Object node	Open / Add to New Project / Add to Existing Project	Editing Restrictions in library security profile*.
	Catalog	Command Restrictions in library security profile*.
	Stow	Command Restrictions in library security profile*.
	Execute	Command Restrictions in library security profile*.
	Rename	Command Restrictions in library security profile*.
	Delete	Command Restrictions in library security profile*.
	Copy	Option "Co" (Copy) "from library" for object type in SYSMAIN utility profile.
	Paste	Option "Co" (Copy) or "Mo" (Move) "from library" for object type in SYSMAIN utility profile.

* or special link security profile

** These actions can be made unavailable in the context menu of the library node by the option "Disable Rename and Delete of Library Node" (described in the section *Administrator Services*).

Location in Server View	Action	Controlled by
DDM node	Open / Add to New Project / Add to Existing Project	Option "List" in SYSDDM utility profile. (*)
	Copy	Option "Co" (Copy) "from library" for DDM in SYSMAIN utility profile.
	Paste	Option "Co" (Copy) or "Mo" (Move) "to library" for DDM in SYSMAIN utility profile.
Object node	Open / Add to New Project / Add to Existing Project	Option "Edit" in SYSDDM utility profile. (*)
	Stow	Option "Cat" in SYSDDM utility profile. (*)
	Cat	Option "Cat" in SYSDDM utility profile. (*)
	Delete	Option "Delete" in SYSDDM utility profile. (*)
	Edit	Option "Edit" in SYSDDM utility profile. (*)

(*) If no SYSDDM utility profile is defined, the Command Restrictions in the SYSDDM *library* profile apply.

Note:
With the current version, the DDMs listed under the DDM node are those related to the user's default library.

Protecting the Eclipse Navigator View

The use of the following actions in the Eclipse Navigator view can be protected by the following Natural Security definitions:

Location in Navigator View	Action	Controlled by
Project node	Upload	Option "Co" (Copy) "to library" for object type in SYSMAIN utility profile.
	Update Server	Option "Co" (Copy) "to library" for object type in SYSMAIN utility profile, and STOW command in Command Restrictions in library security profile*.

* or special link security profile

Disallowed actions are not disabled in the context menus of the Navigator view; the appropriate Natural Security restrictions are only evaluated when the user attempts to perform an action.