Functional Security

This section covers the following topics:

- Command Processors
- Functional Security for a Command Processor
- Allowing/Disallowing Keywords
- Defining Functional Security for a Library
- Defining Functional Security for a User
- Functional Security for Library SYSSEC

Command Processors

Command processors are used to control the way in which commands/functions are executed in a library. They are created with the Natural utility SYSNCP . In a command processor, you define commands - that is, keywords and combinations of keywords - and the actions to be performed in response to these commands being entered by the users.

Functional Security for a Command Processor

Natural Security allows you to define *functional security* for each command processor in a library: you can determine which of the keywords and keyword combinations defined in the processor are to be allowed or not allowed in the library, thus restricting the availability of certain functions within the library. Moreover, you can define user-specific functional security; that is, you can make different functions available for different users of the same command processor in a library.

This is done via the "Functional Security" options in the security profiles of libraries and users, as described in detail in this section. The functional security defined for a command processor in a library profile applies to all users of the command processor in that library. In addition, in a user profile you can define different functional security for an individual user of a command processor in a library, which then takes precedence over the specifications in the library profile.

Status of a Command Processor

In Natural Security, a command processor can have the following status:

Undefined	The command processor has been created with SYSNCP, but no functional security is defined for it.
Defined	The command processor has been created with SYSNCP and functional security is defined for it.
Modified	The command processor has been modified with SYSNCP after functional security was defined for it. In this case, you may have to update the functional security for the command processor; this is done by marking the field "Functional Security Defined" with "UP" and then adjusting the security specifications. To update the functional security for *all* "modified" command processors in the library, you can use the application programming interface NSCLI (function code "UC"). **Note:** If a command processor is modified with SYSNCP, it has to be recataloged in order for the modifications to be reflected in Natural Security.
Unresolved	The command processor has been deleted with SYSNCP, but functional security is still defined for it. In this case, you should also delete the functional security for the command processor (by marking the field "Functional Security Defined" with "DE").

Allowing/Disallowing Keywords

By default, all keywords defined in a command processor are disallowed, which means that none of the commands defined in the processor can be executed.

If you wish to make only relatively few functions available, you can leave this default unchanged so that generally all keywords are disallowed, and you can then allow the use of individual keywords and keyword combinations (commands). If you wish to make most functions available and only restrict the use of relatively few functions, you can change the default so that generally all keywords are allowed and you can then disallow the use of individual keywords and keyword combinations.

Defining Functional Security for a Library

If you mark the option "Functional Security" in the Additional Options window of a library security profile (see "Components of a Library Profile" in the section *Library Maintenance*), the Functional Security window will be displayed:

```
   Library ID ................... XYZLIB__
   Command Processor ............ ________

__ Functional security defined ..
__ Keyword default ..............
__ Keyword exceptions ...........
__ Command exceptions ...........
   Type of command exceptions ...
```

In this window, you can define functional security for any command processor that has been created in that library.

In the Command Processor field of the window, you enter the name of the processor you wish to define for the library.

If you do not know the name of the processor you want, enter an asterisk (*) in the Command Processor field: a list of all processors that are contained in that library will be displayed; from the list, you select a processor by marking it with any character or the cursor.

By default, no functional security is defined for a command processor: the Keyword Default is set to "Disallowed", and no Keyword Exceptions or Command Exceptions are defined; which means that none of the commands defined in the processor can be executed.

Functional Security Defined

This field may take the following values:

No	This indicates that the default settings for Keyword Default and Keyword/Command Exceptions apply.
Yes	This indicates that some of the default settings have been changed.
???	This indicates that the status of the command processor is either "modified" or "unresolved" (see Status of a Command Processor above).

Keyword Default

This field may take the following values:

Disallowed	By default, all keywords specified in the processor are disallowed (and you may allow individual keywords and keyword combinations via Keyword Exceptions and Command Exceptions).
Allowed	By default, all keywords specified in the processor are allowed (and you may disallow individual keywords and keyword combinations via Keyword Exceptions and Command Exceptions).

To change the value from "Disallowed" to "Allowed", or vice versa, mark the Keyword Default input field with any character.

You can only change the Keyword Default if neither Keyword Exceptions nor Command Exceptions are defined; so, if necessary, you must reset the allowed/disallowed status of all Command Exceptions and Keyword Exceptions to their default settings (as explained below) before you can change the Keyword Default.

Keyword Exceptions

This field may take the following values:

No	This indicates that the Keyword Default applies to all keywords; that is, all keywords are either allowed or disallowed.
Yes	If the Keyword Default is set to "Disallowed", this indicates that individual keywords are allowed; if the Keyword Default is set to "Allowed", this indicates that individual keywords are disallowed.

By default, all keywords are either allowed or disallowed, depending on the setting of the Keyword Default.

To change this default status for individual keywords, mark the Keyword Exceptions input field with any character(s) - except "DE". Depending on the Keyword Default, either the Allow Keywords screen or the Disallow Keywords screen will be displayed, listing all keywords that have been defined in the processor:

```
14:18:03                    *** NATURAL SECURITY ***                 2008-10-31
                             - Disallow Keywords -

Library .. SYRINX      Command Processor .. PROC2112

Keyword           Type   A/D
________________ ______  _
ACCESS           Action  A
ADD              Action  A
ADDMULTIPLE      Action  A
ADMIN            Action  A
CONVERT          Action  A
COPY             Action  D
DELETE           Action  D
DISPLAY          Action  A
DUMMY1           Action  A
DUMMY2           Action  A
DUMMY3           Action  A
DUMMY4           Action  A
EDIT             Action  A


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip                                Canc
```

The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

In the "A/D" column, mark the keywords to be disallowed with "D" and those to be allowed with "A".

Any status that is different from the Keyword Default status will be displayed intensified.

To reset the disallowed/allow status of all keywords to the Keyword Default setting, mark the Keyword Exceptions input field with "DE" (delete). A window will be displayed, in which you enter "Y" to confirm the deletion.

Command Exceptions

This field may take the following values:

No	This indicates that all initial default settings apply.
Yes	This indicates that individual default settings have been changed.

If any of the keywords that make up a command is disallowed, the command will, by default, be disallowed. If all of the keywords that make up a command are allowed, the command will, by default, be allowed.

To change this default status for individual commands, mark the Command Exceptions input field with any character(s) - except "DE". The Allow/Disallow Commands screen will be displayed, listing all commands that have been defined in the processor:

```
14:19:13                    *** NATURAL SECURITY ***                  2008-10-31
                          - Allow/Disallow Commands -

Library .. SYRINX      Command Processor .. PROC2112

Action           Object           (unused)         A/D
_______________ _______________ _______________  _
ACCESS           DATASET                          A
ACCESS           JOB                              A
ACCESS           NODE                             A
ACCESS           OPERATIONS                       A
ACCESS           PRINTER                          A
ACCESS           VOLUME_SERIAL                    A
ACCESS           VTAM_APPLICATION                 A
ADD              DATASET                          A
ADD              FILE                             A
ADD              JOB                              A
ADD              LIBRARY                          A
ADD              MAILBOX                          A
ADD              NODE                             A


Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  PrevM Exit  AddOp       Flip                              Canc
```

The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

In the "A/D" column, mark the commands to be disallowed with "D" and those to be allowed with "A".

Any status that is different from the default status will be displayed intensified.

To reset the status of all commands to their default allowed/disallowed settings, mark the Command Exceptions input field with "DE" (delete). A window will be displayed, in which you enter "Y" to confirm the deletion.

Type of Command Exceptions

If any Command Exceptions are defined, this field may take the following values:

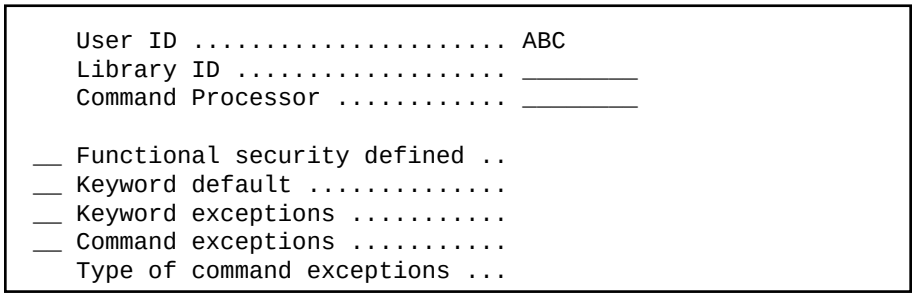
Allowed	This indicates that one or more of the commands that were initially disallowed have been allowed.
Disallowed	This indicates that one or more of the commands that were initially allowed have been disallowed.
Allowed/ Disallowed	This indicates that one or more of the initially disallowed commands have been allowed and also one or more of the initially allowed commands have been disallowed.

Defining Functional Security for a User

Generally, the functional security defined for a command processor in a library security profile applies to all users of the processor in that library. If you wish to define different functional security for an individual user, you may do so in the user's security profile. The specifications in the user profile will then take precedence over the specifications in the library profile.

By default, the functional security specifications as defined for the processor in the library security profile apply.

To change any of these specifications for an individual user, mark the option "Functional Security" in the Additional Options window of the user's security profile (see "Components of a User Profile" in the section *User Maintenance*); the Functional Security window will be displayed:



In this window, you can define user-specific functional security for a command processor in a library.

In the Library ID field of the window, enter the ID of the library in which the processor is contained, and in the Command Processor field, enter the name of the command processor you wish to define for the user.

Functional Security Defined

This field may contain the following values:

No	This indicates that for this user the functional security as defined for the processor in the library security profile applies.
Yes	This indicates that for this user functional security different from that defined for the processor in the library security profile has been defined.
???	This indicates that the status of the command processor is either "modified" or "unresolved" (see Status of a Command Processor above).

To reset the user-specific specifications to those as defined for the processor in the library profile, mark the Functional Security Defined input field with "DE" (delete). A window will be displayed, in which you enter "Y" to confirm the deletion.

Keyword Default/Keyword Exceptions/Command Exceptions/Type of Command Exceptions

For these fields, the same applies as described under *Defining Functional Security for a Library* above.

Functional Security for Library SYSSEC

The command processor NSCCMD01 is provided for the Natural Security library SYSSEC.

Natural Security *always* uses this command processor for the handling of functions within SYSSEC. As SYSSEC would ignore any command processor other than NSCCMD01, it would be useless to create any other command processor for it.

By default, NSCCMD01 is defined with Keyword Default set to "Allowed" and no Keyword Exceptions or Command Exceptions; that is, all Natural Security functions are allowed.

You cannot modify command processor NSCCMD01 itself (as it is only provided in object form). However, if desired, you can control the use of functions within SYSSEC by modifying the functional security aspects of NSCCMD01 in the library profile of SYSSEC and in the user profiles of Natural Security administrators.

For example, if you wish an administrator to only look at security profiles but not modify them, you would disallow for that administrator all action keywords but "DISPLAY"; or, if you wish an administrator to only deal with security profiles of users, but not security profiles of any other type of object, you would disallow for that administrator all object keywords but "USER".

The keywords in NSCCDM01 correspond to the Natural Security commands as listed under *Direct Commands* in the section *Finding Your Way In Natural Security*.

Warning:
Do not set the Keyword Default for command processor NSCCMD01 to "Disallowed" - unless you define *immediately* afterwards Keyword Exceptions that allow you to use all the Natural Security functions you need. If you set the Keyword Default for NSCCMD01 to "Disallowed" and then leave the Functional Security window, all Natural Security functions would be disallowed; that is, no one would be able to use Natural Security anymore. To make Natural Security accessible again, it would then be necessary to execute an INPL with the RECOVER option.