

Natural for Mainframes

Natural Security

Version 4.2.6 for Mainframes

October 2009

This document applies to Natural Version 4.2.6 for Mainframes and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © Software AG 1979-2009. All rights reserved.

The name Software AG, webMethods and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA, Inc. Other company and product names mentioned herein may be trademarks of their respective owners.

Table of Contents

1 Natural Security	1
2 Structure And Terminology Of Natural Security	3
Users	4
Libraries	9
Links Between Users and Libraries	10
DDMs/Files	10
Utilities	12
Applications	12
RPC Servers	12
Other Object Types	13
Profile Parameters	13
3 Natural Security On Different Platforms	15
Supported Platforms	16
Using Natural Security on Multiple Platforms	17
4 Logging On	21
Logon Procedure	22
LOGON Command	25
Automatic Logon	27
How to End a Natural Session	28
5 Finding Your Way In Natural Security	29
Invoking a Function	30
Pressing the ENTER Key	31
Help	31
Not Sure What to Enter?	31
Handling a List	31
Direct Commands	36
6 Administrator Services	43
Access to Administrator Services	45
General Options	45
PF-Keys	62
Logon/Countersign Errors	64
Logon Records	68
Maintenance Log Records	70
SAF Online Services	77
User Default Profiles	81
Library Default Profiles	82
Library and User Preset Values	84
Definition of System Libraries	92
Definition of Undefined Libraries	92
7 User Maintenance	95
Before You Begin	96
Components of a User Profile	96
Creating and Maintaining User Profiles	105

8 Library Maintenance	119
Components of a Library Profile	120
Creating and Maintaining Library Profiles	145
9 Protecting Libraries	155
Protected Libraries	156
Linking Users to Libraries	158
Which Conditions of Use are in Effect?	162
10 Protecting Environments	165
Concept of Environment Protection	166
Activation of Environment Protection	166
Defining Environment Profiles	167
Components of an Environment Profile	168
Disallowing/Allowing Access to Libraries in Environments	171
Disallowing/Allowing Users Access to Environments	173
11 Protecting DDMs On Mainframes	177
Before You Begin	178
Components of a File Profile	179
Creating and Maintaining File Profiles	183
12 Protecting DDMs On UNIX, OpenVMS And Windows	191
Status of a DDM	192
DDM Security Profiles	196
Creating and Maintaining DDM Security Profiles	199
Add DDM Profile	200
Copy DDM Profile	201
Modify DDM Profile	201
Delete DDM Profile	201
Display DDM Profile	202
Copy Link to All Special Links	202
Linking a Library to a Protected DDM	203
13 Protecting Utilities	205
General Utility Protection Considerations	206
Which Utilities Can Be Protected?	206
Utility Profiles	207
Defining Default Profiles	218
Defining Individual Profiles - Utility Maintenance	220
Components of Utility Profiles	227
Conversion of Utility Profiles	241
14 Protecting the Natural Development Server Environment and Applications	245
Protecting the Natural Development Server Environment	246
Protecting Natural Development Server Applications	251
15 Protecting the Natural for Eclipse Environment	271
Protecting the Natural Server View for Eclipse	272
Protecting the Eclipse Navigator View	275
16 Protecting Natural RPC Servers and Services	277
RPC Service Requests	278

RPC Server Settings in Natural	278
RPC Server Settings in Natural Security	279
Validation of an RPC Service Request	280
Security Profiles for Natural RPC Servers	285
Components of an RPC Server Profile	286
Creating and Maintaining RPC Server Profiles	290
IAF Support	294
Other RPC-Related Features	297
17 Protecting External Objects	299
Types of External Objects	300
IDs for External Objects	301
Components of an External Object's Security Profile	301
Creating and Maintaining External Object Security Profiles	304
Linking Users to External Objects	309
18 Mailboxes	315
What is a Mailbox?	316
Broadcasting a Message	316
Receiving a Message	317
Mailbox ID	318
Components of a Mailbox Profile	318
Creating and Maintaining Mailbox Profiles	320
19 Retrieval	325
Purpose of Retrieval Functions	326
Invoking Retrieval Functions	326
Cross-Reference User	327
Cross-Reference Library	328
Cross-Reference File	328
Cross-Reference Utility	329
Cross-Reference Application	329
Cross-Reference External Object	329
Cross-Reference Mailbox	330
Retrieval in Batch Mode - Program RETRIEVE	330
20 Countersignatures	333
Using Owners	334
Using Countersignatures	334
Groups as Owners	336
Groups as Co-Owners	337
User Security Profiles of ADMINISTRATORS	337
Deferred Countersigning	338
Inaccessible Security Profiles	340
21 Functional Security	341
Command Processors	342
Functional Security for a Command Processor	342
Allowing/Disallowing Keywords	343
Defining Functional Security for a Library	343













Defining Functional Security for a User	347
Functional Security for Library SYSSEC	348
22 Natural Security In Batch Mode	351
General Information on Batch Mode	352
Logon in Batch Mode	352
Batch User Security Profiles	354
Countersignatures in Batch Mode	355
23 Transferring Security Data To Another System File	357
General Information on Security Data Transfer	358
Using SECULD2	359
Using SECLOAD	361
Transferring Data to Another Hardware Platform	362
Transferring Data in Batch Mode	363
24 User Exits	367
Logon-Related User Exits	368
RPC-Related User Exit	370
Other User Exits	371
25 Application Programming Interfaces	373
Overview of Subprograms	374
Subprogram NSC---L	376
Subprogram NSC---P	376
Subprogram NSC---SP	377
Subprogram NSC---P	377
Subprogram NSCADM	378
Subprogram NSCCHCK	378
Subprogram NSCDA	379
Subprogram NSCDA-C	379
Subprogram NSCDA-P	379
Subprogram NSCDA-S	380
Subprogram NSCDAU	380
Subprogram NSCDAUC	380
Subprogram NSCDAUP	381
Subprogram NSCDAUS	381
Subprogram NSCDEF	381
Subprogram NSCDU	382
Subprogram NSCFI	382
Subprogram NSCLI	383
Subprogram NSCMA	384
Subprogram NSCOB	385
Subprogram NSCUS	386
Subprogram NSCUT	387
Subprogram NSCXLO	388
Subprogram NSCXR	388
Subprogram NSCXRIER	393
Subprogram NSCXRUSE	393














Subprogram SECNOTE	394
26 Add-On Products and Plug-Ins	395
Plug-Ins under Natural Security	396
SYSDIC under Natural Security	397
SYSAOS under Natural Security	398
Index	401

1 Natural Security

This documentation describes all functions and aspects of usage of Natural Security. It applies to Natural Security on all supported platforms.

This documentation is intended for users of Natural Security, that is, users who are to be defined in Natural Security as users of type ADMINISTRATOR. The reader is assumed to be familiar with and have a good general understanding of Natural.

	Structure And Terminology Of Natural Security	Basic concepts of Natural Security.
	Natural Security On Different Platforms	Considerations for the use of Natural Security on different platforms, and the differences between these platforms.
	Logging On	Rules that apply when a user logs on to Natural under Natural Security.
	Finding Your Way In Natural Security	Various aspects of handling the Natural Security user interface.
	Administrator Services	Descriptions of the functions of the Administrator Services section of Natural Security.
	User Maintenance	User security profiles, their components, and the functions used to create and maintain them.
	Library Maintenance	Library security profiles, their components, and the functions used to create and maintain them.
	Protecting Libraries	How to control the access of users to protected libraries.
	Protecting Environments	How to make library protection environment-specific.
	Protecting DDMs On Mainframes	How to control the use of DDMs on mainframe computers.
	Protecting DDMs On UNIX, OpenVMS And Windows	How to control the use of DDMs on UNIX, OpenVMS and Windows.
	Protecting Utilities	How to control the use of Natural utilities.

	Protecting the Natural Development Server Environment and Applications	How to control the use of the Natural Development Server environment, and Natural Development Server base applications and compound applications.
	Protecting the Natural for Eclipse Environment	How to control the use of the server and navigator views used by Natural for Eclipse.
	Protecting Natural RPC Servers and Services	How to control the use of Natural remote procedure calls in a client/server environment.
	Protecting External Objects	How to control the use of external objects.
	Mailboxes	How to create, maintain and use mailboxes.
	Retrieval	How to review the existing security profile definitions and their effects.
	Countersignatures	How Natural Security administrators control each other.
	Functional Security	How to restrict the availability of functions and make different functions available for different users.
	Natural Security In Batch Mode	How to use Natural Security in batch mode.
	Transferring Security Data To Another System File	How to transfer Natural Security data from one system file to another.
	User Exits	Information on the available user exits.
	Application Programming Interfaces	The subprograms for performing Natural Security functions from outside the Natural Security library SYSSEC.
	Add-On Products And Plug-Ins	Considerations for the protection of various add-on products and plug-ins.

For information on how to install Natural Security, see the Natural *Installation* documentation.

For information on changes, enhancements and new features provided with the current version, see the Natural *Release Notes*.



Caution: If you have multiple versions of Natural Security on a shared FSEC system file, you should use only the latest version for the maintenance of your security data. If you maintain the data with an older version, the consistency of the data cannot be guaranteed, particularly as far as items introduced with later versions are concerned.

2 Structure And Terminology Of Natural Security

■ Users	4
■ Libraries	9
■ Links Between Users and Libraries	10
■ DDMs/Files	10
■ Utilities	12
■ Applications	12
■ RPC Servers	12
■ Other Object Types	13
■ Profile Parameters	13

This section describes the basic concepts of Natural Security. It covers the following topics:

Natural Security is a comprehensive system to control and check the access to a Natural environment. Natural Security enables you to protect your Natural environment against unauthorized access and improper use.

You may define exactly who will be allowed to do what. You may restrict the use of whole libraries and Natural utilities, as well as individual programs, functions and DDMs. You may further define the conditions and times of use. Thus you may provide a custom-made Natural environment for each individual user.

This is accomplished by defining objects and the relationships between these objects. An object is defined to Natural Security by creating a *security profile* for it.

There are four main types of objects which can be defined under Natural Security:

- users
- libraries
- DDMs/files
- utilities

Users

Users can be either people or terminals - or groups of people and/or terminals - who use Natural under Natural Security. When a user is defined, a *user type* classification has to be made. This classification pre-determines the user's possibilities of using libraries.

People may be defined as one of the following user types:

- MEMBER
- PERSON
- ADMINISTRATOR

Terminals may be defined as the user type:

- TERMINAL

Users of the above types may be joined in groups which will be defined as the user type:

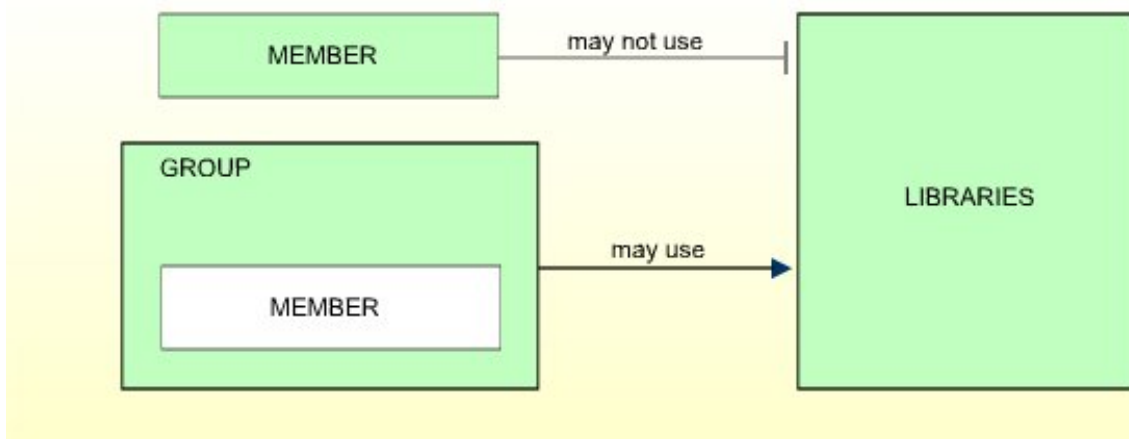
- GROUP

In addition, the following user type is available for usage in batch mode:

- BATCH

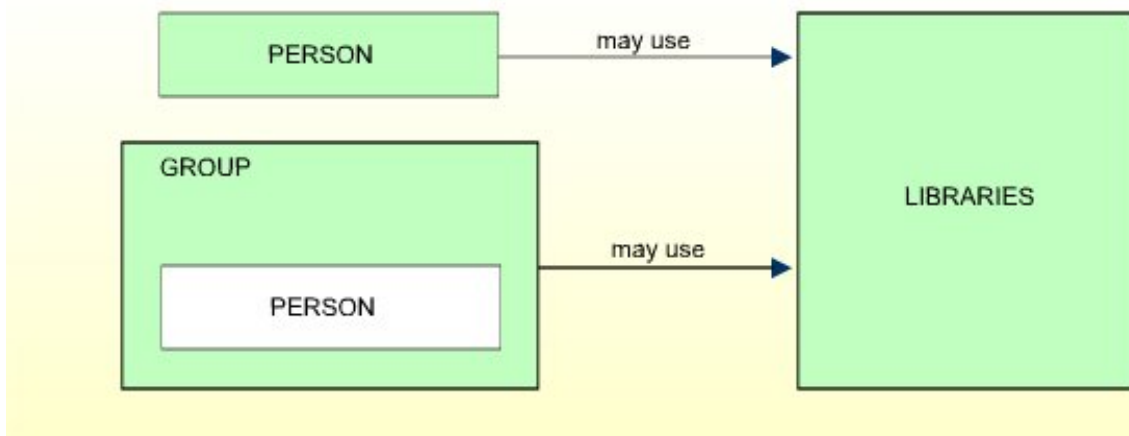
User Type MEMBER

MEMBERS cannot use libraries directly. They may only use libraries through membership in GROUPs. Therefore they have to be assigned to at least one GROUP so as to be able to use any library. Normally, this is the standard user type which will apply to most people.



User Type PERSON

PERSONs may use libraries directly. They may also be assigned to GROUPs. Thus, they may use libraries either directly or through membership in GROUPs. This user type is designed for people who are to have special, individually defined access rights to libraries.

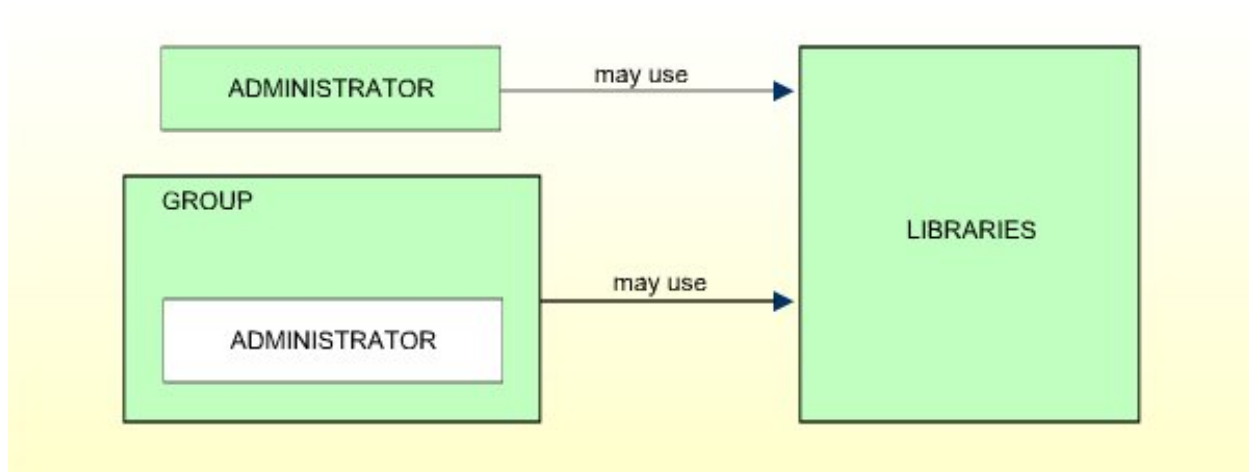


User Type ADMINISTRATOR

ADMINISTRATORs may use libraries directly. They may also be assigned to GROUPs. Thus, they may use libraries either directly or through membership in GROUPs. In this respect they are like PERSONs.

However, only ADMINISTRATORs may maintain Natural Security, that is, create and modify the security profiles of objects and the relationships between these objects.

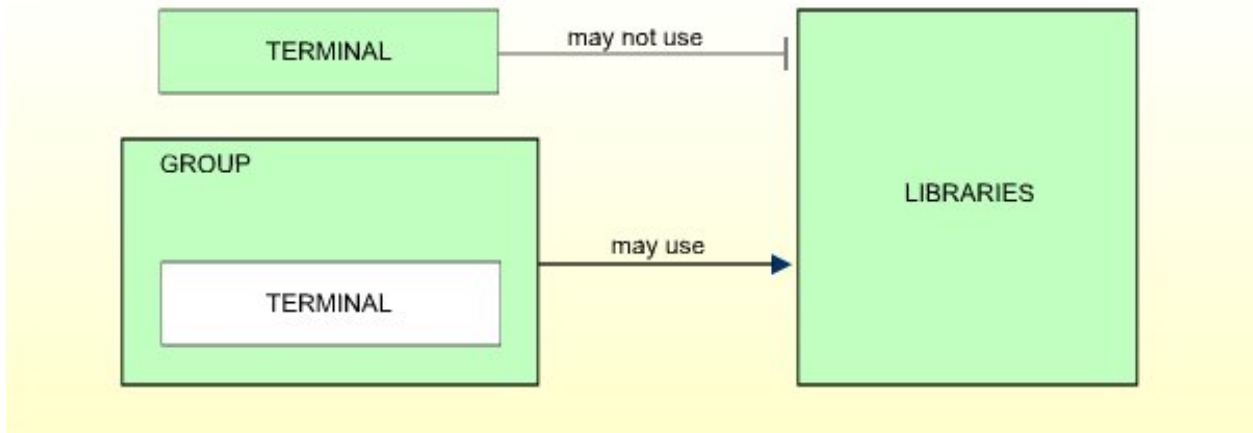
This user type is only for those users who are to be system administrators of Natural Security.



User Type TERMINAL

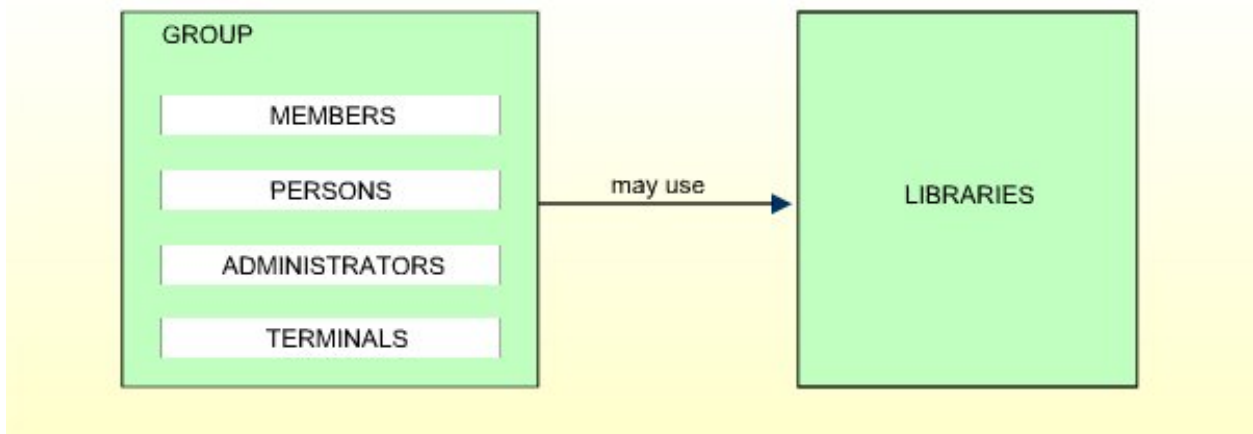
This user type applies to terminals only. Terminals do not necessarily have to be defined. The definition of terminals becomes relevant only in connection with libraries which are to be used from certain terminals only.

TERMINALs cannot use libraries directly, but only through membership in GROUPs. Therefore, TERMINALs have to be assigned to at least one GROUP.



User Type GROUP

GROUPs may be created to allow easier Natural Security maintenance. A GROUP may contain users of any of the other user types. However, a GROUP must not contain another GROUP. Users may be contained in more than one GROUP.



Access rights to libraries may be defined for a GROUP and will then apply for all users contained in the same GROUP, thus saving the effort of having to define them for each user individually. (For ADMINISTRATORs and PERSONs contained in GROUPs, individual access rights different from those of the GROUPs they are in may optionally be defined.)

User Type BATCH

The user type BATCH only applies in batch mode, and is only used if users are to use Natural under different conditions in batch mode than online.

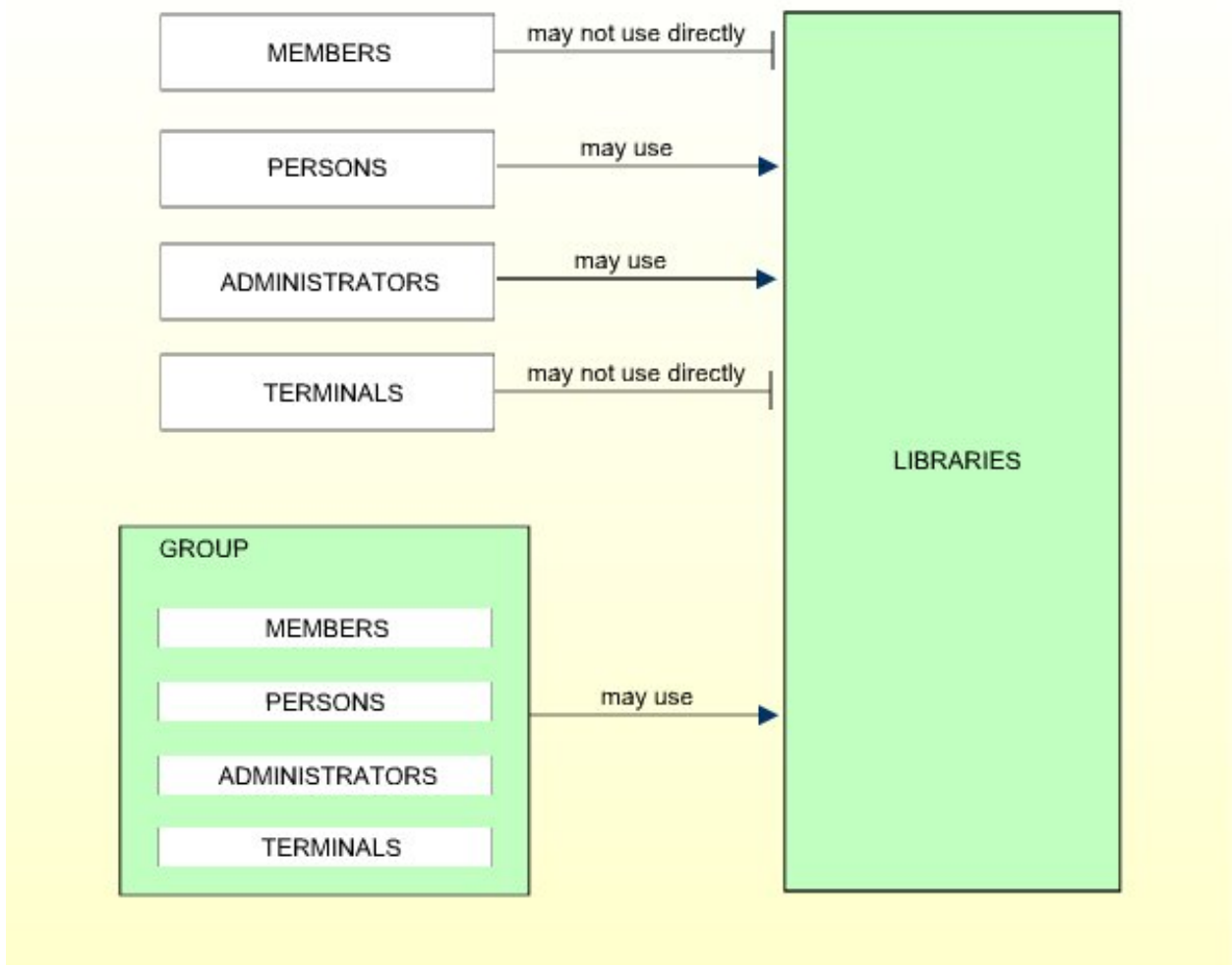
It cannot be compared directly with the other user types, and is only mentioned here for the sake of completeness. For details on this user type, see [Batch User Security Profiles](#) in the section *Natural Security In Batch Mode*.

Which User Type for Which User?

It is generally best to initially define all people as MEMBERS. If need be, a MEMBER may at a later stage be changed to a PERSON. MEMBERS and PERSONs may be “promoted” to become ADMINISTRATORS.

Every user should be assigned to at least one GROUP. It is recommended that GROUPs be used as much as possible, as this will not only reduce Natural Security maintenance considerably, but also provide for a more consistent protection setup.

To recapitulate, the user types basically differ from each other as far as their access to libraries is concerned. The possible relationships are summarized in the following diagram:



Libraries

Libraries are Natural libraries which contain sets of source programs and/or object modules which perform a particular function.

Libraries may be defined as *protected* or *unprotected*.

Unprotected Libraries

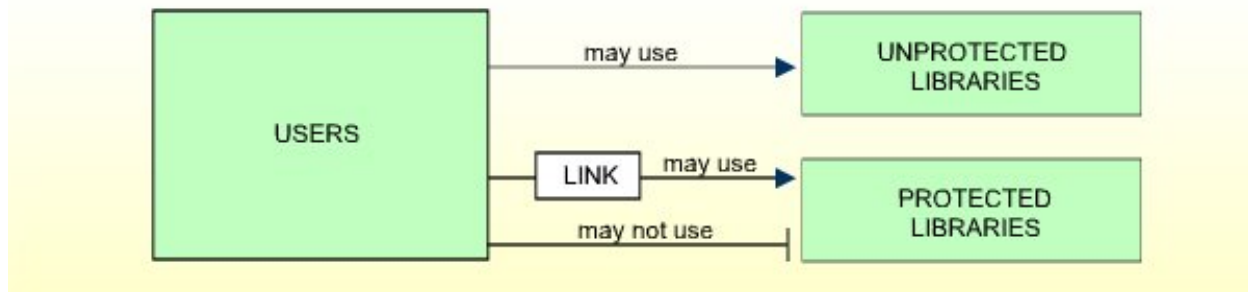
These may be used by any user without a special relationship having to be defined. (Remember that only users of type ADMINISTRATOR or PERSON may use libraries directly. MEMBERS and TERMINALS may use libraries only through membership in a GROUP.)

Protected Libraries

These may be used only by users who have a special relationship to the libraries. This special relationship is called *link*.

Links Between Users and Libraries

A *link* is the relationship between a user (user type ADMINISTRATOR, PERSON, or GROUP) and a protected library which allows the user to use the library.



The various types of library protections and links to libraries are described in the section [Protecting Libraries](#).

DDMs/Files

The protection of DDMs is different depending on the platform you use. This is because with Natural on non-mainframe platforms, DDMs are stored in libraries, whereas with Natural on mainframe computers, DDMs are stored in an FDIC system file and not directly related to a library. See also the section [Natural Security On Different Platforms](#).

On mainframe computers, a DDM must be defined as a *file* to Natural Security before it can be used under Natural Security, that is, a so-called *file security profile* must be created for the DDM. On non-mainframe platforms, a *DDM security profile* is created, which is subordinate to the security profile of the library containing the DDM.

For every DDM, a *status* classification has to be made in Natural Security. This status determines if the DDM can be used, that is, referenced in a database access statement within a Natural program.

File Status on Mainframes

On mainframes, a DDM has only one *file status* (which is set in its file security profile), which may be one of the following:

PUBLIC	The DDM is not protected. It can be used - that is, read and updated - by any library.
ACCESS	The DDM is protected as far as update is concerned. It can be read by any library. It may, however, be updated only by libraries which have been <i>linked</i> to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been <i>linked</i> to it. Such a link may be defined as “read” (that is, read only) or “update” (which implies read).

For details, see the section [Protecting DDMs On Mainframes](#).

Internal and External Status on Non-Mainframes

On non-mainframe platforms, a DDM has an *internal status* and an *external status*.

The internal status controls the use of the DDM *within* the library in which it is contained. It may be one of the following:

PUBLIC	The DDM can be read and updated by all programs within the library.
ACCESS	The DDM can be read, but not updated, by all programs within the library.
PRIVATE	The DDM cannot be used by any program within the library.

The external status controls the use of the DDM by *other* libraries - provided that the library containing the DDM is used as a steplib by other libraries. It may be one of the following:

PUBLIC	The DDM is <i>not</i> protected. It can be used - that is, read and updated - by any library.
ACCESS	The DDM is protected as far as update is concerned. It can be read by any library. It may, however, be updated only by libraries which have been <i>linked</i> to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been <i>linked</i> to it. This <i>link</i> may be defined as “read” (that is, read only) or “update” (which implies read).

For details, see the section [Protecting DDMs On UNIX, OpenVMS And Windows](#).

Utilities

With Natural Security, you can control the use of various Natural utilities. This utility protection is function-oriented, which means that you can allow or disallow the functions of a utility individually.

You control the use of a utility by defining *utility profiles* for it. Various types of hierarchically layered utility profiles allow you to define exactly who will be allowed to use which function.

Moreover, for utilities which affect the contents of individual libraries, you can determine for which libraries a utility function is to be allowed and for which not. This, you can also define differently for individual users.

For details, see the section [*Protecting Utilities*](#).

Applications

Applications are *base applications* and *compound applications*, which are created and maintained in the Natural Studio's application workspace and used in conjunction with the Natural Development Server.

If the Natural Development Server is installed at your site, you can control the access to base and compound applications with Natural Security. To do so, you define security profiles for the applications and establish links between users and applications.

For details, see the section [*Protecting Natural Development Server Applications*](#).

RPC Servers

In a client/server environment, you can use Natural Security to protect the use of Natural remote procedure calls. You can protect Natural RPC servers as well as the way in which Natural RPC *service requests* issued by clients are handled by these servers.

To control the access to Natural RPC servers and their handling of service requests, Natural Security provides several options to be set; in addition, you can define security profiles for Natural RPC servers to be protected.

For details, see the section [*Protecting Natural RPC Servers and Services*](#).

Other Object Types

Apart from users, libraries, DDMs/files, utilities and applications, there are other types of objects which can be defined under Natural Security. However, these other objects are not essential for protecting your Natural environment with Natural Security. Other object types are:

- **External Objects:**

These are objects of various types which are used by Predict and other products (see the section [External Objects](#) for details).

- **Mailboxes:**

These are information screens which may be used to broadcast messages to Natural users (see the section [Mailboxes](#) for details).

Profile Parameters

Several Natural profile parameters are influenced by Natural Security. The following list provides an overview of these profile parameters and their corresponding settings in Natural Security.

Profile Parameter	Corresponding Setting in Natural Security
CF	CF in Session Parameters section of library profiles.
CLEAR	CLEAR in Session Parameters section of library profiles.
DC	DC in Session Parameters section of library profiles.
DU	DU in Session Parameters section of library profiles.
EJ	EJ in Session Parameters section of library profiles.
ETA	"Error" in Transactions section of library profiles.
ETID	"Default ETID" in user profiles.
FS	FS in Session Parameters section of library profiles.
FUSER	The settings in the Library File section of library profiles.
IA	IA in Session Parameters section of library profiles.
ID	ID in Session Parameters section of library profiles.
IM	IM in Session Parameters section of library profiles.
LS	LS in Session Parameters section of library profiles.
LT	"Processing loop limit" in Security Limits section of library profiles.
MADIO	"Maximum number of Adabas calls" in Security Limits section of library profiles.
MAXCL	"Maximum number of program calls" in Security Limits section of library profiles.
MT	"Maximum amount of CPU time" in Security Limits section of library profiles.
OPRB	"Adabas open" in Session Parameters section of library profiles.

Profile Parameter	Corresponding Setting in Natural Security
PS	PS in Session Parameters section of library profiles.
RPC	The settings in the Natural RPC Restrictions section of library profiles.
SA	SA in Session Parameters section of library profiles.
SF	SF in Session Parameters section of library profiles.
SL	SL in Session Parameters section of library profiles.
SLOCK	SLOCK in Session Parameters section of library profiles.
SM	“Programming Mode” in General Options section of library profiles.
STEPLIB	“Steplibs” in Additional Options section of library profiles
TD	“ Time Differential ” in user profiles.
ULANG	“ Language ” in user profiles.
WH	WH in Session Parameters section of library profiles.
ZD	ZD in Session Parameters section of library profiles.

3

Natural Security On Different Platforms

■ Supported Platforms	16
■ Using Natural Security on Multiple Platforms	17

This section covers the following topics:

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](#)

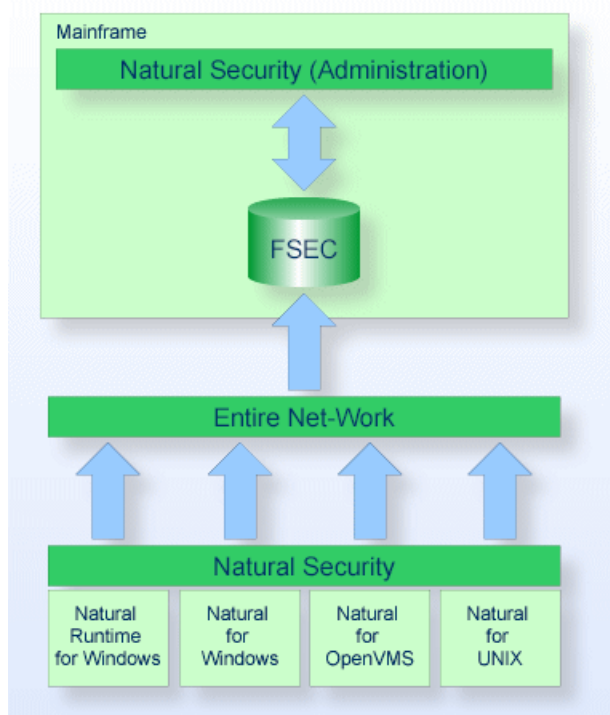
Central FSEC System File

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 NATCONFIG.
- 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.

4

Logging On

■ Logon Procedure	22
■ LOGON Command	25
■ Automatic Logon	27
■ How to End a Natural Session	28

This section describes the rules which apply when a user logs on to Natural under Natural Security. It covers the following topics:

Logon Procedure



Note: If a user invokes Natural under Natural Security and the FNAT system file specified in the parameter file/module used is a non-Security system file, Natural cannot be started, and the user will receive an appropriate error message.

The logon procedure is used by Natural Security to ensure that the user who is logging on to Natural is authorized for the library requested.

A logon must be executed successfully before any Natural session can be started.

A logon screen (on mainframe computers, under UNIX and OpenVMS) or logon dialog box (under Windows) is provided for the user to enter the information required for the logon.

Logon Screen / Logon Dialog Box

When Natural Security is installed, the Natural Security logon screen will be displayed whenever a user invokes Natural.

Under Windows, the logon screen is displayed as a dialog box (for the sake of consistency, however, it will also be referred to as “logon screen”).

The logon screen requests the user to enter the following:

Library ID	<p>The ID of the library to be used.</p> <p>To determine which libraries are available, the user may enter his/her user ID in the user ID field and an asterisk (*) in the library ID field: a list of all libraries available to the user will be displayed. The list contains all non-protected libraries and all protected libraries to which the user is linked (either directly, or via a group whose security profile is activated). The list also contains all libraries available to the user's terminal (if the terminal is defined to Natural Security. To view a list of all libraries available to the terminal, the user may enter an asterisk (*) in the library ID field without entering a user ID.)</p> <p>Note: For a logon from the Natural Studio in a client environment via the Natural Development Server to a Map Environment on a mainframe server, the specification of an asterisk (*) as library ID is not possible.</p>
User ID	<p>The ID by which the user is defined to Natural Security.</p> <p>The ID of a group must not be entered; a terminal ID must not be entered either.</p>

	If no user ID is entered, Natural Security will use the ID of the terminal being used. In this case the terminal has to be defined to Natural Security; otherwise the logon will be rejected.
Password	The password specified in the user's security profile. If no password has been specified in the user's security profile, the password will be identical to the user ID (when a newly defined user logs on for the first time and the password is identical to the user ID, the user must change his/her password by entering a new password in the New Password field).
New Password	If a valid password has been entered in the Password field and the user wishes/has to change that password, the user enters a new password in this field. This new password will then replace the old password and will from then on be the valid password for the user.

The following rules apply for entering values on the logon screen:

- If a user ID is entered, a password must also be entered.
- If no user ID is entered, no password is required.
- A new password can only be entered if a valid password is entered as well.

Passwords

In a user's security profile, the Natural Security administrator may change the password, and may also set a time interval, after which the user will be forced to change the password. The user will then have to enter a password and a new password to be able to log on (for details on these options, see the section [User Maintenance](#)).

If a user has forgotten his or her password, he/she will have to contact the Natural Security administrator, who may then specify a new password in the user's security profile. This will then be the valid password for the user (which he/she may change again in the logon screen).

A password or new password when entered will not be displayed on the screen.

Logon Customization

You can customize the logon screen / logon dialog box to suit your requirements:

- **Mainframe computers, UNIX and OpenVMS:**
The source code of the logon screen, map NOGONM1, is provided in the library SYSSEC. To customize the logon screen, you make a copy of NOGONM1, store it under the name LOGONM1, modify it to suit your requirements, catalog it, and then copy the cataloged object LOGONM1 into the library SYSLIB. Should LOGONM1 be missing from SYSLIB, the Natural Security installation procedure will automatically copy the object module NOGONM1 from SYSSEC to SYSLIB and store it there under the name LOGONM1; this ensures that a default logon screen is always present if no customized one is used.

■ **Windows:**

The same applies as described above for the logon screen - except that the names for logon dialog box are different: The source provided in the library SYSSEC is called GNOGONM1, and the object to be copied into the library SYSLIB is called GLOGONM1.

There are also logon-related user exits available, which may be used to customize the logon procedure (see [Logon-Related User Exits](#) in the section User Exits).

Rejected Logon

A logon to a library will be rejected if:

- the user is not defined to Natural Security;
- the user's security profile is currently inactive (due to Activation Dates settings);
- the user is defined as user type MEMBER and has not been assigned to a group;
- the user is defined as user type MEMBER, and the security profile of the group to which he/she is assigned is currently inactive (due to Activation Dates settings);
- the library is not defined to Natural Security;
- the time window restrictions defined in the library's security profile do not permit use of the library at the time of the logon;
- the library is protected and the user is not linked to the library;
- the library is protected and the user is linked to it, but the link has been temporarily locked;
- the library is protected, and the group via which the user is linked to the library is currently inactive (due to Activation Dates settings in the group security profile);
- a non-existent startup transaction is specified in the library's security profile;
- the NEXT/MORE line is not allowed nor a startup transaction specified in the library's security profile.

Logon Without Library ID

If no library ID is entered in the logon screen, the default library specified in the user's security profile will be invoked.

If no default library is specified in the user's security profile, the "Privileged Groups" specified in the user's security profile will be checked (in order of entry) for a default library.

If none of the Privileged Groups has a default library either, the user's **private library** will be invoked.

If neither default libraries nor a private library exist, the user must enter a library ID when he or she logs on.

RESTART and FIN as Library IDs

If “RESTART” is entered as the library ID, the last RESTARTable library to which the user was logged on will be invoked (for details on the “RESTART” option, see [Transactions](#) in the section Library Maintenance).



Note: The ID of the last RESTARTable library to which a user was logged on is shown in the field “Last Library” in the user security profile.

If “FIN” is entered as the library ID, the Natural session will be terminated.

Successful Logon

After a successful logon to a library the following may be invoked:

- the startup transaction specified in the library's security profile (if specified);
- the Natural main menu, if no startup transaction is specified.



Note: Internally, Natural Security performs an `END OF TRANSACTION` statement after a successful logon if any of the following applies:

- the user's password has been changed during the logon procedure;
- a logon error has occurred during the logon procedure;
- the “Logon recorded” option in the user's or the library's security profile is set to “Y”;
- the “Restart” option in the library profile is set to “Y”;
- the “Lock User Option” in the General Options (Administrator Services) is set to “X”.

LOGON Command

If the first logon to a library at the beginning of a Natural session was successful, a user may change from one library to another by using the Natural system command LOGON.

See also the Natural *System Commands* documentation for information on the LOGON system command.

The LOGON command takes the following parameters:

- If no parameter is specified, the default library will be invoked (either the user's or one of the privileged group's); if no default library is specified, the Natural Security logon screen will be invoked. For example:

```
LOGON
```

- If one parameter is specified, it will be interpreted as a library ID. For example:

```
LOGON LIBX
```

```
LOGON *
```

- If two parameters are specified, the first will be interpreted as a user ID, the second as a password. For example:

```
LOGON USERX PASSWX
```

- If three parameters are specified, the first will be interpreted as a library ID, the second as a user ID, the third as a password. For example:

```
LOGON LIBX USERX PASSWX
```

- If four parameters are specified, the first will be interpreted as a library ID, the second as a user ID, the third as a password, the fourth as a new password. For example:

```
LOGON LIBX USERX PASSWX NEWPASSX
```

LOGON Command Errors

If an error is detected during logon processing, Natural Security will display an error message.

If the LOGON command has been invoked from a library, Natural Security will invoke the error transaction defined for the library. If no error transaction is defined, the logon screen will be invoked.

Automatic Logon

Users would normally have to log on twice, first to the operating system and second to Natural. To eliminate the need for a second logon, you may set the Natural profile parameter AUTO to AUTO=ON (which is described in the *Natural Parameter Reference* documentation).

As a result, an internal Natural Security logon procedure will be invoked, which uses the operating-system login name (as contained in the Natural system variable *INIT-USER) as the user ID, but no password (on the assumption that this has been verified by the operating-system logon procedure). The Natural Security logon screen will be suppressed. A logon with a user ID other than the operating-system login name will not be possible.

If AUTO=ON is used, the user has no possibility of specifying a library ID. The library to which the user will be logged on is determined by the same rules as described under [Logon Without Library ID](#) above. This means that automatic logon is only possible if a default library is specified (for the user or one of his/her Privileged Groups) or the user has a private library.

If you combine AUTO=ON with specifying a default library in a user's security profile and with specifying a startup transaction for that library, the user will receive the first screen of the default library immediately after invoking Natural without having to pass any intermediate screens (default libraries are described under [Components of a User Profile](#) in the section *User Maintenance*, startup transactions under [Transactions](#) in the section *Library Maintenance*).

If AUTO=ON is set, the system command LOGOFF has the same result as the system command FIN (see [How to End a Natural Session](#) below).

If AUTO=ON is set, and after the initial automatic logon the user tries to log on to another library and causes a logon error, the error transaction for the current library will be invoked. If no error transaction is specified, an error message will be issued and then the startup transaction (if specified) for the current library will be invoked.

How to End a Natural Session

The following Natural system commands may be used to end a Natural session under Natural Security:

LOGOFF	<p>This command terminates a Natural session and invokes the logon screen. To leave the logon screen, you enter "FIN" as the library ID.</p> <p>If the profile parameter AUTO=ON is set (see Automatic Logon above), the LOGOFF command has the same effect as the FIN command.</p>
LOGON (without parameters)	<p>This command terminates a Natural session and starts the logon procedure, invoking either a default library or the logon screen (if no default library is defined).</p> <p>See also Automatic Logon above.</p>
FIN	<p>This command terminates a Natural session and is used to leave Natural altogether.</p>



Caution: Natural Security cannot protect your Natural environment against unauthorized use if Natural users leave their terminals unattended whilst being logged on to Natural. Therefore, users should be reminded to use the LOGOFF command before they leave their terminal. Unauthorized persons will then be confronted with the Natural Security logon screen and may only use what has been defined for them to use under Natural Security.

In library security profiles, you can specify a non-activity time limit, after which a logoff will be executed automatically.

5

Finding Your Way In Natural Security

■ Invoking a Function	30
■ Pressing the ENTER Key	31
■ Help	31
■ Not Sure What to Enter?	31
■ Handling a List	31
■ Direct Commands	36

This section provides information on handling Natural Security. It covers the following topics:

Invoking a Function

You can invoke Natural Security functions from within the Natural Security library SYSSEC or from outside of SYSSEC.

Within SYSSEC:

- You can invoke a function by selecting it from a Natural Security menu or [selection list](#).
- You can invoke a function by issuing a [direct command](#).

Outside of SYSSEC:

- You can invoke a function via one of the [application programming interfaces](#) provided.
- You can invoke a function by issuing a [direct command](#).

Profile Security

Regardless of how you invoke a function, Natural Security's administrator/owner settings will always apply; that is, you can only apply functions to those security profiles you are allowed to maintain.

Functional Security

All SYSSEC-specific commands are defined in the command processor NSCCMD01. You can disallow Natural Security functions by disallowing the corresponding commands in NSCCMD01. For details on NSCCMD01, see the section [Functional Security for Library SYSSEC](#).

If functions are disallowed in NSCCMD01, the corresponding menu items will not be visible on the Natural Security menus. This means that within SYSSEC you only see the functions you are allowed to use.

Aborting a Function

Do not use the Natural terminal command "%%" to abort a Natural Security function, as this may cause inconsistencies in your Natural Security data.

Pressing the ENTER Key

To tell Natural Security to perform a particular action, you enter the appropriate function code, command, etc. and then press the ENTER key.

So, if the Natural Security documentation tells you to "enter a function code", this means, "type in the function code and press ENTER".

If a function requires that you press another key, this is explicitly mentioned in the Natural Security documentation.

Help

To invoke online help for a Natural Security function:

- you enter a question mark (?) as a function code on screens with a function code input field; or
- you press PF1 on any Natural Security screen.

An explanation of a given screen and the information necessary to proceed will be displayed.



Note: If certain items displayed on a Natural Security screen are not directly relevant for the execution of the function concerned, these items are not always explained in this documentation. In these cases, you will find the corresponding explanations in the online help.

Not Sure What to Enter?

If you are not sure what you can enter in an input field on a Natural Security menu or selection screen, enter an asterisk (*) in the field: a window will be displayed showing you all the possible values for the field; in the window, you can then select the desired value.

Handling a List

This section covers the following topics:

- [Selecting the Range of Objects to be Listed](#)
- [Scrolling a List](#)

- [Selecting an Object from a List](#)

Selecting the Range of Objects to be Listed

When you invoke the Maintenance or Retrieval subsystem for a certain object type (user, library, etc.), a list of these objects will be displayed. Normally such a list will contain all objects.

For example, to list all users defined to Natural Security, you mark object type “User”.

```
+-----MAINTENANCE-----+
! Please select one type of object: !
!                                     !
! X User                             !
! _ Application                       !
! _ Library                          !
! _ File                             !
! _ Mailbox                          !
! _ Utility                          !
!                                     !
!                                     !
! Start Value .. _____          !
! Type/Status .. _____          !
+-----+
```

The contents of the above selection window may vary depending on the platform and the types of external objects available. If the list of object types exceeds the size of the window, you can use PF7 and PF8 to scroll within the window.

If you do not want a list of all objects but would like only certain objects to be listed, you may use the option “Start Value”.

For users, applications, libraries and files, you may also use the option “Type/Status” - either alone or in combination with the “Start Value” option. For other objects, only the “Start Value” option is available.

Start Value

In this field you may enter a start value, which may consist of one or more characters, or of one or more characters followed by an asterisk (*). The option to enter a value followed by an asterisk is referred to as *asterisk notation* throughout the Natural Security documentation.

For example, to list all users, starting from the first user whose ID begins with “TOM”, you mark object type “User” and enter the following:

```
Start Value .. TOM
```

For example, to list only those users whose IDs begin with “TOM”, you mark object type “User” and enter the following:

```
Start Value .. TOM*
```

Type/Status

In this field you may enter a user type, application type, library protection status, or (on mainframes) a file status.

User Type

User type may be one of the following:

G	Group
M	Member
P	Person
A	Administrator
T	Terminal
B	Batch User

Library Protection Status

Library protection status may be one of the following:

NN	Not protected.
LN	Not protected, but linkable for one group.
YN	People-protected only.
NY	Terminal-protected only.
YY	People- or terminal-protected.
YA	People- and terminal-protected.
PN	For private libraries: same as “YN”.
PY	For private libraries: same as “YY”.
PA	For private libraries: same as “YA”.

(The above **protection combinations** are explained in the section *Protecting Libraries*.)

File Status

File status may be one of the following:

PRIV	Private.
ACCE	Access.
PUBL	Public.
UNDF	Undefined; that is, DDMs for which no file security profiles have been created (*).
DEFI	Defined; that is, all PRIV, ACCE, and PUBL files (*).
NDDM	File security profiles for which no DDMs exist (*).
DDM	All PRIV, ACCE, PUBL and UNDF files (*)

* This is not an actual file status, but for selection purposes only.

If you do not select a file status, all PRIV, ACCE, and PUBL files will be listed.

Application Type

Application type may be one of the following:

B or BASE	Base applications.
C or COMP	Compound applications.

If you do not select an application type, both base and compound applications will be listed.

Example of Type/Status option:

To list all users of user type “Member”, you mark object type “User” and enter the following:

```
Type/Status .. M
```

Example of combining Start Value and Type/Status:

To list only users of user type “Member” whose IDs begin with “T”, you mark object type “User” and enter the following:

```
Start Value .. T*
Type/Status .. M
```

Scrolling a List

Once a list of objects is displayed, you may scroll it backwards and forwards in the following manner:

- To scroll a list one page forward, you press PF8 (+).
- To scroll a list one page backward, you press PF7 (-).
- To scroll a list to its beginning, you press PF19 (- -).
- To scroll a list to a specified start value, you may use the *intensified* field above the IDs, in the same way as described above for the Start Value field.
- For a list of users or applications, you can also use the *intensified* field above the Type column in the same way as described above for the Type/Status field. For a list of libraries, the same is true for the field above the Protection Status column. These fields display the currently valid type/status selection criterion.

```
11:38:39                *** NATURAL SECURITY ***                2009-07-31
                        - User Maintenance -

Co User ID  User Name                                Type Message
---
___ AAZ      ABDUL ALHAZRED                            A
___ AD       ARTHUR DENT                                A
___ AH       ALICE HARGREAVES                          M
___ ER       ELLEN RIPLEY                              M
___ LL       LOCKE LAMORA                                M
___ TN       THURSDAY NEXT                              A
___ VV       VINCENT VEGA                              P
```

Selecting an Object from a List

To select an object from a list for a function, you simply type in the appropriate function code for the function next to the object in the left-hand column (entitled “Co”) of a selection screen.

If you do not remember the function code for the function you wish to perform, enter an asterisk (*) in the “Co” column. A window will be displayed which shows all the function codes available; in the window, you can then select the desired function code.

Direct Commands

This section covers the following topics

- [General Command Information](#)
- [Commands to Invoke a Function](#)
- [Commands to Invoke a Selection List](#)
- [Special Commands](#)
- [Issuing a Command Outside of SYSSEC](#)

General Command Information

Once you are familiar with Natural Security and know how to find your way from menu to menu, you may be interested in invoking the function you want directly. This is done by using *direct commands*.

You can enter a direct command on any Natural Security screen which provides a *command line*:

```
Command ==>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help      Exit                                  Canc
```

If you enter a direct command which is invalid, you will receive an appropriate error message. If you enter a command which is incomplete, you will be prompted to specify the missing item(s).

After a function invoked by a direct command has been executed, the screen from which that function would “normally” be invoked will be displayed - *not* the screen on which the command had been entered.

There are three types of direct commands:

- **commands to invoke a function,**
- **commands to invoke a selection list,**
- **special commands.**

Commands to Invoke a Function

General Command Syntax

Generally, a direct command which is used to invoke a function consists of the following components, which you specify in the following order:

function object-type object-ID parameters

First, you specify a *function*. Possible functions are:

ADD	Add security profile.
COPY	Copy security profile.
MODIFY	Modify security profile.
RENAME	Rename security profile.
DELETE	Delete security profile.
DISPLAY	Display security profile.
EDIT	Edit group members.
LINK	Link object to another object.
XREF	Cross-reference object.

After the function, you specify an *object-type* (for example, USER, LIBRARY).

After the object type, you can specify an *object-ID* (for example, a user ID or library ID).

After the ID, you can specify one or more *parameters* (for example, a user type).

Parameters for Security-Profile Components

For the functions DISPLAY and MODIFY, several *parameters* are available which allow you to directly access those components of a security profile which are not on the main security-profile screen, but on one of profile's Additional Options screens. These are:

For all *object-types*:

Parameter	Security-Profile Component
DIR	Maintenance Information.
NOTES	Security Notes.
OWNERS	Owners.

For *object-type* USER:

Parameter	Security-Profile Component
MAILBOXES	Mailboxes.
ACTIVATION	Activation Dates.
FUNCSEC	Functional Security.
PRIVLIB	Private Library (only for user types A and P).
SESSION	Session Options (only for user types A and P).

For *object-type* LIBRARY:

Parameter	Security-Profile Component
MAILBOXES	Mailboxes.
TIMEW	Time Windows.
STEPLIBS	Steplibs.
FUNCSEC	Functional Security.
USEREXIT	User Exit.
OPTIONS	Security Options.
LIMITS	Security Limits.
PARAMETERS	Session Parameters.
RPC	Natural RPC Restrictions.
COMMANDS	Command Restrictions.
EDITORS	Editing Restrictions.
STATEMENTS	Statement Restrictions.
MODULES	Disallow/Allow Modules.
DDMSTATUS	Set Status of DDMs.

Abbreviating a Command

You may abbreviate the *function* component of a direct command as you please, as long as the abbreviation uniquely identifies the function.

You may abbreviate the *object-type* component of a direct command to 2 characters.

Examples:

DISPLAY USER ADE	This command causes the security profile of user "ADE" to be displayed.
DISPLAY US ADE DIS USER ADE DI US ADE	Each of these three commands also causes the security profile of user "ADE" to be displayed.
DE US ADE	This command invokes the Delete function for user "ADE".
D US AE	This command is <i>invalid</i> , because "D" does not uniquely identify a function; it could stand for DISPLAY or DELETE.

Several Natural system commands are available within Natural Security; they must also be taken into consideration as far as the unique identification of a function is concerned.

Command Examples

ADD	If you enter this command on a Maintenance selection list, the Add function for that type of object will be invoked. If you enter it somewhere else, the command is incomplete, because no object type was specified.
ADD US	The Add User window will be invoked for you to enter a user ID and user type.
ADD US CMOT	The Add User window will be invoked for you to enter a user type.
ADD US CMOT M ANKH	The Add User screen for user "CMOT" of user type "Member", using default profile "ANKH" as the basis of the user profile to be created, will be invoked for you to define the user.
MODIFY	This command is incomplete, because no object type was specified after the function.
MODIFY LIB	This command displays the Library Maintenance selection list, as no library ID was specified.
MOD LIB BOOKS	The security profile of library "BOOKS" will be displayed for modification.
CO US ESME	The Copy User window will be displayed for you to enter the user ID of the new user.
CO US ESME OGG	The Copy User screen for user "OGG" will be invoked with the security profile of user "ESME" copied into the security profile of user "OGG". The copying is without links.
CO US ESME OGG Y	The Copy User screen for user "OGG" will be invoked with the security profile of user "ESME" copied into the security profile of user "OGG". The copying is with links.
EDIT US DOC	Invokes the Edit Group Members function for the group "DOC".

XREF MAIL MAIL1	Invokes the Cross-Reference function for mailbox “MAIL1”.
LK LI ODDS US	The Link Users To Library screen will be invoked for users to be linked to library “ODDS”; the list will contain all users.
LINK US IW LI	The Link User To Libraries screen will be invoked for user “IW” to be linked to libraries; the list will contain all libraries.

Commands to Invoke a Selection List

The following commands can be used to invoke a selection list:

Command	Function
<u>MAINTENANCE</u> <i>object-type</i> <i>object-ID</i> <i>parameters</i>	<p>If you specify only the command itself, the object selection window for maintenance functions will be displayed.</p> <p>If you specify an <i>object-type</i> after the command, the Maintenance selection list for that type of object will be displayed.</p> <p>If you specify an <i>object-type</i> and an <i>object-ID</i> after the command, the Maintenance selection list for that type of object will be displayed, and the <i>object-ID</i> will be used as start value for the list.</p> <p>After the <i>object-ID</i>, you can specify one or more <i>parameters</i> (for example, user type) as further selection criteria for the Maintenance selection list to be displayed.</p>
<u>RETRIEVAL</u> <i>object-type</i> <i>object-ID</i> <i>parameters</i>	<p>If you specify only the command itself, the object selection window for retrieval functions will be displayed.</p> <p>In the same manner as for the MAINTENANCE command (see above), you can specify an <i>object-type</i>, <i>object-ID</i> and <i>parameters</i> with this command.</p>

Special Commands

Apart from commands which invoke a particular function or selection list (as described above), and several Natural system commands (which are described in the *Natural System Commands* documentation), the following special commands are available (underlining indicates the shortest abbreviation possible):

Command	Function
<u>ADMIN</u>	Invokes the Administrator Services Menu.
ADMIN_D	Invokes the Administrator Services function Library And User Preset Values .
ADMIN_I	Invokes the Administrator Services function Application Programming Interfaces .
ADMIN_N	Invokes the Administrator Services function Maintenance Log Records .

Command	Function
ADMIN_S	Invokes the Administrator Services function Definition of System Libraries .
ADMIN_U	Invokes the Administrator Services function User Default Profiles .
ADMIN_X	Invokes the Administrator Services function Utility Defaults/Templates .
ADMIN_Y	Invokes the Administrator Services function Library Default Profiles .
ADMIN_1	Invokes the Administrator Services function Environment Profiles .
ADMIN_3	Invokes the Administrator Services function Definition of Undefined Libraries .
CONVUTIL	Invokes the function for the conversion of utility profiles .
CUSTOM1 CUSTOM2 CUSTOM3 CUSTOM4 CUSTOM5	These commands invoke Natural programs of the same names. You can write your own programs of these names to perform whatever functions you require; this allows you to invoke such functions from within Natural Security.
ERRDEL	Deletes all logon/countersign error entries (see also Deleting All Error Entries - Direct Command ERRDEL in the section <i>Administrator Services</i>).
ERROR	Invokes the Logon/Countersign Errors Menu.
LOGDEL	Deletes all logon records (see also Deleting All Logon Records - Direct Command LOGDEL in the section <i>Administrator Services</i>).
LOGFILE	Invokes the Administrator Services function Log File Maintenance .
LOGREC	Invokes the Logon Records Menu.
MENU	Invokes the Natural Security Main Menu.
. (period)	Terminates the given processing level and displays the screen of the next higher processing level (the same as PF3).

Issuing a Command Outside of SYSSEC

You can also issue a Natural Security direct command from outside of the Natural Security library SYSSEC. This allows you to perform a Natural Security function from anywhere in your Natural session without having to log on to the library SYSSEC.

To do so, you enter the direct command - prefixed by SYSSEC - in the Natural command line.

For example:

```
SYSSEC MOD LIB XYZ
```

When you leave the screen invoked by the direct command, you will be returned to the Natural screen from which you have issued the command.



Note: When you issue a direct command which invokes a function, you have to specify the full command, that is, you must not omit any command component necessary to invoke the actual function (and not only a selection screen or start-value window). For example, the command COPY USER ABC would be incomplete, because the new user ID is missing.

6 Administrator Services

▪ Access to Administrator Services	45
▪ General Options	45
▪ PF-Keys	62
▪ Logon/Countersign Errors	64
▪ Logon Records	68
▪ Maintenance Log Records	70
▪ SAF Online Services	77
▪ User Default Profiles	81
▪ Library Default Profiles	82
▪ Library and User Preset Values	84
▪ Definition of System Libraries	92
▪ Definition of Undefined Libraries	92

This section covers the following topics:

The Administrator Services subsystem provides several functions which apply to Natural Security as a whole and to all security profiles.

You select “Administrator Services” on the Main Menu. If you have access to the subsystem (see [Access to Administrator Services](#) below), the Administrator Services Menu will be displayed.

The Administrator Services Menu consists of two screens. With PF7 and PF8, you can switch between the two screens. They provide the following functions:

Administrator Services Menu 1:

- [General Options](#) (*)
- [PF-Keys](#)
- [Logon/Countersigns Errors](#)
- [Logon Records](#)
- [Maintenance Log Records](#)
- [SAF Online Services](#)

Administrator Services Menu 2:

- [Environment Profiles](#)
- [User Default Profiles](#) (*)
- [Library Default Profiles](#) (*)
- [Library and User Preset Values](#)
- [Utility Defaults/Templates](#) (*)
- [Definition of System Libraries](#)
- [Definition of Undefined Libraries](#)
- [Application Programming Interfaces](#)

You should study the functions marked above with (*) before you start defining objects to Natural Security. The other Administrator Services functions are not directly related to defining objects to Natural Security.

Access to Administrator Services

As far as access to the Administrator Services subsystem is concerned, the following applies:

- If owners are specified in the security profile of the Natural Security library SYSSEC, only these owners have access to the Administrator Services subsystem.
- If SYSSEC has no owners assigned, every ADMINISTRATOR may access the Administrator Services subsystem.

For information on owners in library security profiles, see the sections [Library Maintenance](#) and [Countersignatures](#).

General Options

Before you start defining objects to Natural Security, it is advisable to specify a number of options which will apply to the Natural Security system as a whole.

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu, you select “General options”. The Set General Options screen will be displayed.

The Set General Options screen consists of two screens. With PF7 and PF8 you can switch between the two screens. They provide the following options:

General Options - Screen 1:

- [Transition Period Logon](#)
- [Activate Security for Development Server File](#)
- [Maximum Number of Logon Attempts](#)
- [Suppress Display of Logon Messages](#)
- [Lock User Option](#)
- [User Password History](#)
- [Free Access to Functions via APIs](#)
- [Minimum Number of Co-Owners](#)
- [Deletion of Non-Empty Libraries Allowed](#)

- **Overwriting of Defaults Possible**
- **Display DBID/FNR of FSEC**
- **Exit Functions with Confirmation**
- **Logging of Maintenance Functions**

General Options - Screen 2:

- **Concurrent Modifications Without Notification**
- **Private Libraries in Public Mode**
- **Suppress Mailboxes in Batch Mode**
- **Environment Protection**
- **Force Impersonation for Natural Development Server**
- **Record Each User's Initial Logon Daily**
- **Enable Error Transaction Before NAT1700/1701 Logoff**
- **Logoff in Error Case if *STARTUP is Active**
- **Set *APPLIC-NAME Always to Library Name**
- **Allow Deletion of Users Who Are Owners/DDM Modifiers**

The individual options are described below.

Transition Period Logon

This option allows a smooth transition from an unprotected Natural environment to one protected by Natural Security.

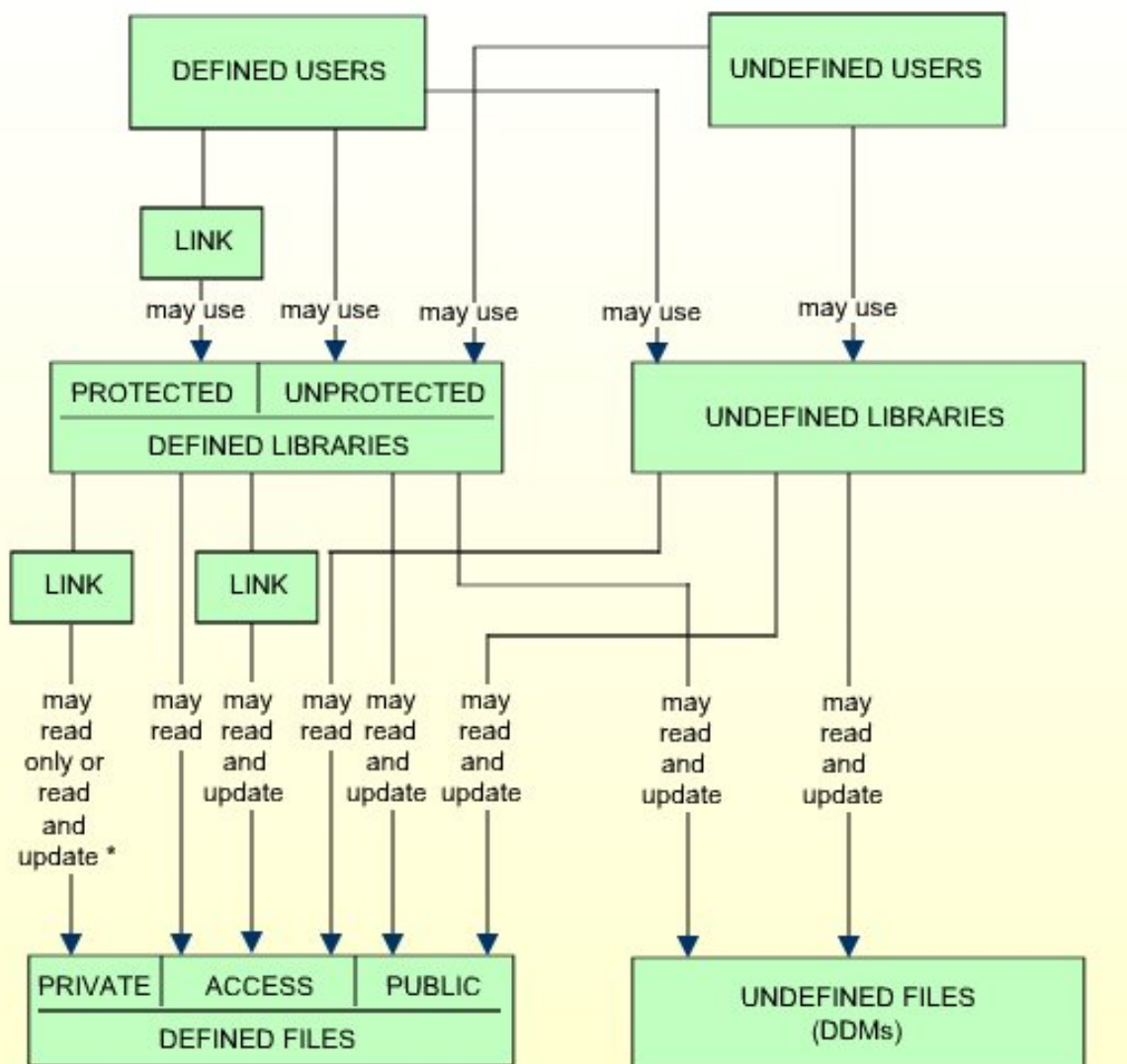
Y	<ul style="list-style-type: none">■ Users not yet defined to Natural Security may log on to libraries which are not yet defined to Natural Security or which are defined as unprotected.■ Libraries not yet defined to Natural Security may be accessed by any (defined or undefined) user.■ Undefined libraries may access DDMs which are not yet defined to Natural Security as well as files of status PUBLIC and ACCESS.■ Undefined DDMs may be accessed by any (defined or undefined) library.
N	Only users defined to Natural Security may use Natural. Any library not defined to Natural Security cannot be used.

The effects of the Transition Period Logon settings are illustrated below.

If you have had an unprotected Natural installation and now have installed Natural Security for the first time, it is advisable to set the Transition Period Logon to “Y” so as to ensure that work

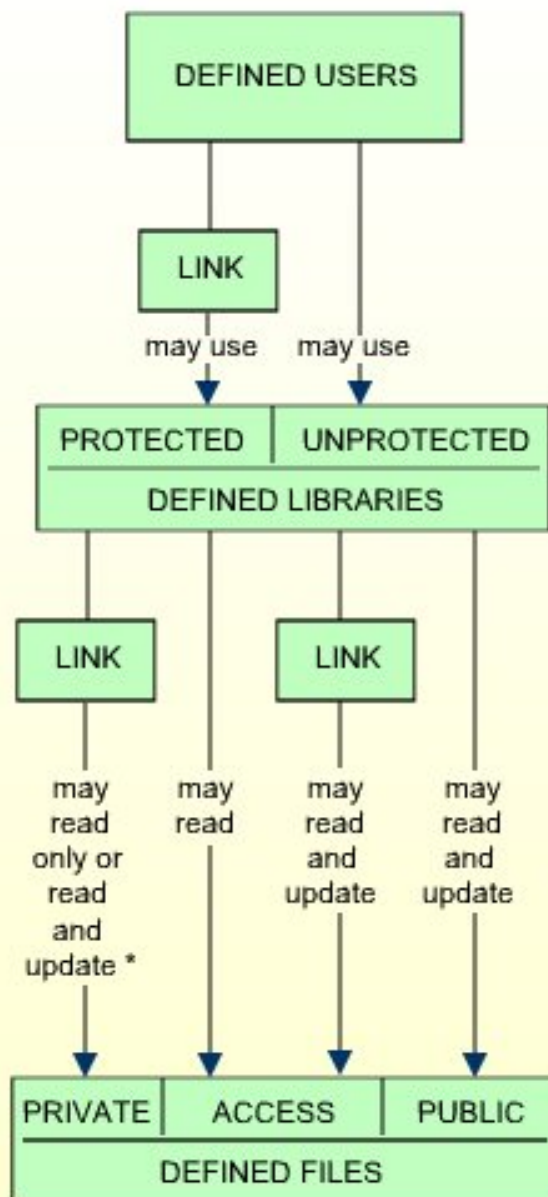
with Natural may continue while users and libraries are defined to Natural Security. Once all objects and links are defined, the Transition Period Logon should be set to “N”.

Conditions of use under Transition Period Logon = Y:



* depending on link specification

Conditions of use under Transition Period Logon = N:



* depending on link specification

Activate Security for Development Server File

This option only appears if the Natural Development Server is installed and the current Natural session uses a development server file. It is only relevant if you wish to control the access to base and compound applications on the development server file. For details, see the section [Protecting Natural Development Server Applications](#).

Y	<p>Security for the development server file is active: The application security profiles for base and compound application defined in Natural Security take effect and control the access to the Natural Development Server objects “base applications” and “compound applications” on the development server file.</p> <p>The FSEC system file which is being used when this option is set to “Y” will be defined to the development server file. This development server file can then only be used in a Natural Security environment. All security checks made by the Natural Development Server in the Natural Studio's application workspace will be performed using the security definitions on that FSEC system file.</p> <p>If you set this option to “Y”, this will also activate Predict Security (if not already activated in Predict, by setting the Predict parameter “Protect Predict File” on the General Defaults > Protection screen to “Y”). Please note that the activation of Predict Security will not only affect the access to base and compound applications, but may also cause other Predict Security settings not related to applications to take effect.</p> <p>The database ID and file number of the development server file for which the option is activated will be shown on the Set General Options screen.</p>
N	<p>Security for the development server file is not active. Application security profiles are not evaluated.</p>

Maximum Number of Logon Attempts

1-5	<p>You may specify how many attempts to log on users shall have. After n unsuccessful logon attempts, the logon procedure will be terminated, the user “thrown out”, and a logon-error record written (for information on logon-error records, see Logon Errors below).</p>
------------	--

Suppress Display of Logon Messages

This option may be used to suppress the display of the messages NAT0853 and NAT0854, which indicate that a logon to a library has been successful. By default, one of these messages is displayed after every successful logon to a library.

Y	Messages NAT0853 and NAT0854 will not be displayed.
N	Messages NAT0853 and NAT0854 will be displayed.

Lock User Option

This option may be used to prevent users from trying to misuse other users' user IDs and passwords. It applies to the logon procedure (see [Logon Procedure](#) in the section *Logging On*) and to the countersignatures feature (see the section [Countersignatures](#)).

Y	<p>Logon:</p> <p>For logon attempts, the following applies: Once a user has reached the maximum number of logon attempts without entering the correct password, the respective user will be locked, that is, the user ID will be made "invalid". The following will be locked:</p> <ul style="list-style-type: none"> ■ all Natural Security user IDs which were tried out, ■ the user's operating-system login name (as identified by the Natural system variable *INIT-USER), if a Natural Security user profile exists whose ID corresponds to that name. <p>Countersignatures:</p> <p>For countersign attempts, the following applies: After too many invalid passwords (the maximum number of logon attempts also applies here) on a Countersign screen, the user who invoked the respective function (as identified by his/her Natural Security user ID) will be locked.</p>
F	<p>Logon:</p> <p>For logon attempts, "F" has the same effects as "Y" - in addition, the Natural session is terminated when the user is locked.</p> <p>Countersignatures:</p> <p>For countersign attempts, "F" has the same effect as "Y".</p>
X	<p>Logon:</p> <p>For logon attempts, "X" has the same effects as "F" - except that Natural Security "remembers" unsuccessful attempts across sessions: With "Y" and "F", the counters of logon attempts for the user IDs which were tried out unsuccessfully is reset when the user aborts the logon procedure. With "X", however, these error counters are kept for logon procedures in subsequent sessions, thus reducing the number of subsequent logon attempts with these user IDs. This means that the chances of someone gaining access with another user's ID are reduced considerably. With "X", the error counter for a user ID is only reset after a successful logon.</p> <p>Countersignatures:</p> <p>For countersign attempts, "X" has the same effect as "Y".</p> <p>A user's error counters can be displayed by pressing PF16 in his/her security profile. A list of all users whose error counters are greater than "0" can be obtained with the application programming interface NSCXRUSE.</p>

N	The Lock User feature is not active.
---	--------------------------------------

Natural RPC Service Calls

For logon attempts to libraries via Natural RPC service calls, this option only takes effect if the “Lock user option” in the [Library And User Preset Values](#) is set to “*”. For Natural RPC service calls, the following applies:

- The settings “Y” and “F” have the same effect as “X”.
- When locking occurs, the client user IDs which are locked will not include the ID as contained in the system variable *INIT-USER.

User Password History

This option may be used to exercise more control over the users' usage of passwords to enforce more efficient password protection.

Y	<p>Password history is active. This has the following effects:</p> <ul style="list-style-type: none">■ The last <i>nn</i> passwords used by each user are recorded by Natural Security. These last <i>nn</i> passwords cannot be used again by the user as new password. You set the number of passwords to be recorded in the window displayed when you activate this option. Possible values: 1 - 99.■ A user is forced to change his/her password at logon when the password has been changed by an administrator in the user's security profile.■ You can define certain rules to which passwords must conform. You define these password rules by using the function “Library and User Preset Values” (see below).
N	Password history is not active.

Other password-related Natural Security features are:

- the minimum password length (see [Library and User Preset Values](#) below),
- the password case-sensitivity (see [Library and User Preset Values](#) below),
- and the password expiration (field "Change after *nnn* days"), which can be set in user security profiles (see the section [User Maintenance](#)).

Free Access to Functions via APIs

You may specify who may access Natural Security maintenance and retrieval functions from outside Natural Security via the application programming interfaces (APIs) provided. For details on these APIs, see the section [Application Programming Interfaces](#).

Y	Maintenance and retrieval functions may be accessed from outside Natural Security via the APIs by anybody who may use the APIs. If you set this option to “Y”, you can protect each maintenance/retrieval function separately using functional security (see the section Functional Security).
R	Retrieval functions (but not maintenance functions) may be accessed from outside Natural Security via the APIs by anybody who may use the APIs. If you set this option to “R”, you can protect each retrieval function separately using functional security (see the section Functional Security).
N	Maintenance and retrieval functions may be accessed from outside Natural Security only by users (of type ADMINISTRATOR) who may also use the Natural Security library SYSSEC. With the APIs, they may only perform those functions they are also allowed to perform within SYSSEC, and only under the same conditions under which they may perform them in SYSSEC.

Maintenance functions are all functions of the subprograms NSCFI, NSCLI, NSCOB and NSCUS - except their Display functions.

Retrieval functions are all functions of the subprograms NSCCHCK, NSCDEF, NSCDU, and NSCXR and of the subprograms whose names begin with “NSCDA”, as well as the Display functions of the subprograms NSCFI, NSCLI, NSCOB and NSCUS.

Minimum Number of Co-Owners

0-3	You may specify the minimum number of co-owners for each owner of a security profile. The number set here will be valid for all security profiles and cannot be modified individually.
------------	---

For an explanation of co-owners, see the section [Countersignatures](#); leave the value set to “0” until you have read that section.

Deletion of Non-Empty Libraries Allowed

This option determines whether a library's security profile can be deleted if the library contains any source or object modules.

Y	A library's security profile can be deleted even if the library contains any source or object modules. When you try to delete a library profile, Natural Security will issue a warning if the library is not empty. This option only affects the deletion of a library's <i>security profile</i> ; the Natural library itself and the modules it contains are not deleted.
N	A library's security profile cannot be deleted as long as the library itself still contains any source or object modules.

Overwriting of Defaults Possible

This option determines whether the values set on the Preset Library And User Values screen may be overwritten in individual security profiles.

Y	The specifications made on the Preset Library And User Values screen may be overwritten in the individual security profiles.
N	The specifications made on the Preset Library And User Values screen cannot be overwritten in any security profile. They will be valid for all libraries/users without exception.

The preset values are described under [Library and User Preset Values](#) below.

Display DBID/FNR of FSEC

This option determines whether the database ID and file number of the current Natural Security system file (FSEC) are to be displayed on the menu and selection screens within the library SYSSEC.

Y	The database ID and file number of the current Natural Security system file (FSEC) will be displayed on the menu and selection screens within the library SYSSEC. They will be displayed in the top right-hand corner below the current date.
N	The database ID and file number of the FSEC file will not be displayed in SYSSEC.

Exit Functions with Confirmation

This option determines how Natural Security reacts when you leave a function by pressing PF2, PF3, PF12 or PF15.

Y	When you leave a function in Natural Security by pressing PF2, PF3, PF12 or PF15, a window will be displayed in which you have to specify whether the modifications you made before pressing the key are to be saved or not or whether you wish to return to the function.
N	When you leave a function by pressing PF2, PF3 or PF15, the modifications you made before pressing the key will be saved. When you leave a function by pressing PF12, the modifications you made before pressing the key will <i>not</i> be saved.

For details on which function is assigned to which key, see the section *PF-Keys* below.

Logging of Maintenance Functions

This option allows you to ascertain who has modified which security profiles and administrator services settings.

"Modify" in this context comprises all maintenance functions applied to a security profile (including Add, Copy, Delete, Link, etc.); it also includes the transfer of a security profile with the programs SECULD2 and SECLOAD.

Y	Log records are written for modifications to security profiles and administrator services settings.
N	Modifications are not logged.

When you set this option to "Y", a window will be displayed in which you can specify the following:

Log file DBID/FNR	<p>The database ID and file number of the file in which the log records are to be stored. This file must have been loaded during the installation process of Natural Security.</p> <p>Note: Once "Logging of Maintenance Functions" has been activated, you cannot change the log file assignment. You have to deactivate the option, before you can assign another database ID or file number.</p>
------------------------------	--

	<p>Should the log file become inaccessible, and prevent you from deactivating the logging of maintenance functions, you can use the Natural system command INPL with code "R" (Recover) and option "A" (Adjust) to change the log file assignment. As parameters for the command you specify the database ID and file number of the current (inaccessible) log file and of its desired new location. Batch-mode input for this operation would be as follows:</p> <pre>//CMSYNIN DD * R,A old-DBID,old-FNR new-DBID,new-FNR .</pre>
Logging even if no actual modification	<p>Y - Modifications are also logged if nothing has actually been changed; that is, if a security profile or administrator services setting has been invoked for modification, but no actual change has been made to the profile/setting.</p> <p>N - Modifications are only logged if a profile/setting has actually been changed.</p>
Logging of changes to	<p>Possible values: N, Y, and (for user and library profiles) X.</p> <p>You mark with "Y" the object types whose modifications are to be logged:</p> <ul style="list-style-type: none"> ■ administrator services settings (*), ■ user security profiles, ■ library security profiles (including special link profiles), ■ file security profiles, ■ application security profiles, ■ mailbox security profiles, ■ various types of external object security profiles. <p>(*) "Administrator services settings" in this context means all functions listed on the Administrator Services Menu (except "Application Programming Interfaces").</p> <p>Utility Profiles</p> <p>Modifications to utility security profiles are not logged separately. Instead, default profiles and templates are handled under "administrator services settings", library-specific utility profiles under "library security profiles", and user-specific and user-library specific utility profiles under "user security profiles".</p> <p>Extended Logging for User and Library Profiles</p> <p>You can mark "user security profiles" and "library security profiles" with "X" (instead of "Y") for the following additional data to be logged.</p> <p>For user security profiles:</p> <ul style="list-style-type: none"> ■ When the Copy User function is used with the "with links" option, any relationship which the copying has established between the user and other objects is logged.

	<ul style="list-style-type: none"> ■ When the Delete User function is used, any relationship which existed between the user and other objects and which was removed by the deletion is logged. <p>For library security profiles:</p> <ul style="list-style-type: none"> ■ When the Copy Library function is used with the "with links" option, any relationship which the copying has established between the library and other objects is logged. ■ When a link between a group and a library is maintained, a list of the group's members is logged. ■ When a maintenance functions affects the Disallow/Modules section of a library (or special link) profile, information on the changed status of any module is logged.
--	---

To change the above specifications once you have activated the writing of log records, you press PF4 on the Set General Options screen.

To view the log records, you use the function **"Maintenance Log Records"** (see below).

Concurrent Modifications Without Notification

This option determines how Natural Security reacts in a situation in which two administrators simultaneously modify the same security profile. Such a situation would occur as follows:

1. Administrator 1 invokes a security profile for modification.
2. Administrator 2 invokes the same security profile for modification.
3. Administrator 1 leaves the function after having made his/her modifications - the modifications are applied to the security profile. This means that, at this point, Administrator 2 is working on data which are "out of date", but is not aware of this fact.
4. Administrator 2 leaves the function after having made his/her modifications. Now there are two possible reactions by Natural Security:
 - The modifications made by Administrator 2 are applied - unknowingly overwriting the modifications made by Administrator 1.
 - Administrator 2 receives a window, informing him/her that the security profile in question was in the meantime modified by another administrator. He/she can then contact the other administrator to discuss the changes made, and can then decide to either cancel his/her own modifications or apply them, thus overwriting the modifications made by Administrator 1.

This option determines which of these two reactions is to be taken; that is:

Y	The modifications will be applied in any case.
N	A window will be displayed in which the administrator can choose to: <ul style="list-style-type: none">■ cancel his/her modifications,■ apply his/her modifications,■ return to the security profile in question.

This option only applies to concurrent modifications made to security profiles of users, libraries, special links and mailboxes.

Private Libraries in Public Mode

This option determines whether private libraries are to be available in “private mode” or in “public mode”.

Y	Private libraries are available in “public mode”.
N	Private libraries are available in “private mode” for exclusive use by the users with the same IDs (not recommended).

See [Private Library](#) in the section *User Maintenance* for further information. Please read that section *before* you set this option.

Suppress Mailboxes in Batch Mode

This option determines whether or not mailboxes are output in batch mode.

Y	Mailboxes are not output in batch mode.
N	Mailboxes are output in batch mode.

For information on mailboxes, see the section [Mailboxes](#).

Environment Protection

This option determines if Natural environments - that is, system-file combinations - are protected.

N	Environments protection is not active: Users can access any environment. Natural Security will not perform any access-authorization checks regarding the environment.
Y	Environments protection is active: Users can only access environments for which security profiles are defined. By default, access to a library in a defined environment is allowed for all users. For individual libraries and users, you can disallow access to an environment.

If you change the setting of this option, you have to restart your Natural session for the change to take effect.

For details on environment protection, see the section [Protecting Environments](#).

Force Impersonation for Natural Development Server

This option is only relevant for the Natural Development Server (NDV). It controls how access to an NDV server is handled.

It is assumed that access to the operating system on which an NDV server is running is controlled by an SAF-compliant external security system. User authentication (verification of user ID and password) is performed by this external security system. After a successful authentication, it generates an “accessor environment element” (ACEE) for the user, which is available for subsequent authorizations.

N	A user can access an NDV server either by using the ACEE generated by the external security system, or directly by using his/her Natural Security user ID and password.
Y	<p>A user can access an NDV server only with the ACEE generated by the external security system. Without an ACEE, access to an NDV server is not possible. This ensures that the external security system's user authentication cannot be bypassed.</p> <p>If the user has an ACEE, no further authentication checks are performed when he/she logs on to the NDV server.</p>

Record Each User's Initial Logon Daily

This option may be used to detect unused user IDs, that is, user security profiles which have not been used for a long time. This may be helpful when you decide to delete user security profiles which are no longer used.

N	Initial logons are not recorded daily.
Y	Each user's initial logon at the start of the Natural session is recorded daily. The date of a user's most recent initial logon is displayed in his/her security profile (by pressing PF16 on the main user profile screen).

When this option is set to Y, you can use the application programming interface **NSCXRUSE** to obtain a list of users who have not logged on since a specified date.

Please note that only logons which occur while this option is active can be recorded.

Enable Error Transaction Before NAT1700/1701 Logoff

This option determines whether or not the current Natural application's relevant **ON ERROR** statement and/or error transaction will be processed in the event of Natural errors NAT1700 (**time window** exceeded) and NAT1701 (**non-activity time limit** exceeded).

The error transaction is determined by the value of Natural system variable *ERROR-TA.

N	When error NAT1700 or NAT1701 occurs, both the application's ON ERROR statements and error transaction will be ignored; Natural Security will perform a logoff, regardless of whether there is any ON ERROR statement or error transaction.
S	When error NAT1700 or NAT1701 occurs, the application's relevant ON ERROR statement will be processed before Natural Security performs a logoff. Any error transaction will be ignored.
E	When error NAT1700 or NAT1701 occurs, the application's error transaction will be processed before Natural Security performs a logoff. Any ON ERROR statement will be ignored.
G	When error NAT1700 or NAT1701 occurs, the application's relevant ON ERROR statement will be processed, and if no ON ERROR statement is encountered, the error transaction will be invoked, before Natural Security performs a logoff.

This option only takes effect on mainframe computers. On non-mainframe platforms, Natural Security always reacts as if it had been set to "G" (regardless of the actual setting).

Logoff in Error Case if *STARTUP is Active

This option determines the course of action to be taken in the case of a Natural runtime error occurring within the ON ERROR condition of a startup transaction (*STARTUP).

When a runtime error occurs within the ON ERROR condition of a startup transaction, Natural's error processing might lead to the startup transaction being executed again. This would cause an error-loop situation. To prevent such a loop, you can set this option.

Y	In the case of a runtime error caused by a startup transaction, a LOGOFF command will be executed at the point when the startup transaction would be due for execution in the course of Natural's error processing.
N	In the case of a runtime error caused by a startup transaction, the Natural system variable *STARTUP will be set to blanks, and Natural's error processing will proceed.

If no startup transaction is defined, this option has no effect.

Set *APPLIC-NAME Always to Library Name

This option determines the value of the Natural system variable *APPLIC-NAME.

Y	*APPLIC-NAME contains the name of the library to which the user is logged on, regardless of whether the user is logged on via a special link or not.
N	*APPLIC-NAME contains the name of the library to which the user is logged on. If the user is logged on via a special link, it contains the special-link name instead.

Allow Deletion of Users Who Are Owners/DDM Modifiers

This option determines whether a user security profile can be deleted if the user is still specified either as owner in any security profile or as DDM modifier in any DDM/file security profile.

This option can only be set if owners are assigned to the Natural Security library SYSSEC.

N	Security profiles of users who are owners or DDM modifiers <i>cannot</i> be deleted. This ensures that the deletion does not cause any undesired owner or DDM modifier constellation.
O	Security profiles of users who are owners or DDM modifiers <i>can</i> be deleted. They can only be deleted by administrators who are owners of the library SYSSEC.
A	Security profiles of users who are owners or DDM modifiers <i>can</i> be deleted. They can only be deleted by the administrator (or group of administrators) whose ID is specified in the field "By Administrator".

If this option is set to "O" or "A" and the security profile of a user is deleted, his/her ID is automatically removed from any security profiles where he/she is specified as owner or DDM modifier. Nonetheless, it may be advisable before the deletion to use the [Cross-Reference User](#) function to

ascertain which profiles/DDMs would be affected, and after the deletion to make sure the changed owner/co-owner and DDM modifier/co-modifier configurations still suit your requirements.

PF-Keys

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu, you select “PF-keys”. The Set PF-Keys screen will be displayed.

On this screen, you can assign functions and names to keys, as described below.

Functions can be assigned to certain keys only. Names can be assigned to all keys.

PF-Key Functions

The functions assigned to the following PF-keys cannot be modified:

Key	Function	Explanation
PF01	Help	If you press PF1 on any Natural Security screen, help information for that screen will be displayed.
PF02	Previous Menu	<p>This key returns you to the menu screen from which you have invoked the current processing level.</p> <p>By default, the modifications you made before leaving a function with PF2 will be saved; see also the general option “Exit Functions with Confirmation” above.</p>
PF03	Exit	<p>This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed.</p> <p>By default, the modifications you made before leaving a function with PF3 will be saved; see also the general option “Exit Functions with Confirmation” above.</p>
PF04	Additional Options	On a security profile screen, you can press this key (instead of marking the Additional Options field on the screen with “Y”) to display the Additional Options selection window for a security profile.
PF05		Various functions on different screens (as described where appropriate).
PF06	Flip	The PF-key lines at the bottom of the Natural Security screens display either PF-keys 1 to 12 or PF-keys 13 to 24. By pressing PF6, you can switch from one display to the other.

Key	Function	Explanation
PF07	Previous Page (-)	This key scrolls a displayed list one page backward.
PF08	Next Page (+)	This key scrolls a displayed list one page forward.
PF12	Cancel	This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed. By default, the modifications you made before leaving a function with PF12 will <i>not</i> be saved; see also the general option “Exit Functions with Confirmation” above.
PF13	Refresh	This key undoes all modifications you have made on a screen but which have not yet been saved. The fields on the screen will be reset to the values they had before you changed them.
PF14		(reserved for future use)
PF15	Menu	This key invokes the Natural Security Main Menu. By default, the modifications you made before leaving a function with PF15 will be saved; see also the option “Exit Functions with Confirmation” above.
PF16 to PF17		Various functions on different screens (as described where appropriate).
PF18		(reserved for future use)
PF19	First Page (- -)	This key scrolls a displayed list to its beginning.
PF20 to PF24		(reserved for future use)



Note: The CLR key has the same function as PF12.

PF09, PF10, PF11, PA1, PA2

You may assign a function to each of these keys yourself. The function assigned will then be invoked within Natural Security by pressing the appropriate PF-key (or PA-key).

One of the following functions may be assigned to a PF-key (or PA-key):

- a Natural system command,
- a Natural terminal command,
- a Natural program.

To assign a function to a key, you enter a command or program name in the “Function” column of the Set PF-Keys screen next to a key number.

PF-Key Names

You may name all PF-keys, including those whose function assignments you cannot change. The names may be up to 5 characters long and can be entered in the "Name" column of the Set PF-Keys screen.

The assigned names will appear in the PF-key lines which are displayed at the bottom of each Natural Security screen:

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

If no name is displayed for a PF-key, this indicates that the function assigned to this key is not applicable to the screen displayed.

The lines display either the keys PF1 to PF12 or the keys PF13 to PF24. By pressing PF6, you can switch from one display to the other, and back again.

Logon/Countersign Errors

The Logon/Countersign Errors functions serve two purposes:

- The Logon Error Processing functions are used to view unsuccessful attempts to log on to Natural.
- The List/Unlock Locked Users function, which is only used in conjunction with the "Lock User Option", is used to view (and unlock) users who have been "locked" due to logon or countersign errors.

Logon Errors

On the Set General Options screen, you can specify the **Maximum number of logon attempts** (see above) by entering a number n in the range from 1 to 5 (the default is 5). Every time a user makes n consecutive unsuccessful logon attempts, the user will be "thrown out" and a *logon error record* will be written by Natural Security. The logon error record contains detailed information on each of the n logon attempts that led to the record being written (for example, which user and library IDs were entered by the user). The records may be viewed by using the Logon Error Processing functions.

Being able to view logon error records serves the following purposes:

- You can ascertain whether unauthorized people have tried to gain access to Natural.
- You can ascertain what users do wrong when they try to log on. Users may then be informed how to log on correctly.

- You can ascertain whether users have been given the appropriate access rights. A user may, for example, try to log on to a library he/she is not (but should be) allowed to use. In this case you may then make the necessary Natural Security maintenance adjustments to the security profiles and relationships concerned.

The recording by Natural Security of logon errors cannot be switched off.

In addition, Natural Security records unsuccessful attempts to access a Natural utility. These utility access error records can also be viewed with the Logon/Countersign Errors functions.



Note: Unless explicitly indicated otherwise, the term “logon errors (records)” as used in the text below also comprises utility access errors (records).

Locked Users

If the **“Lock User Option”** (see General Options above) is active, users may be “locked” due to logon or countersign errors:

- **Logon errors:**
Once a user has reached the maximum number of logon attempts without entering the correct password, the user will be locked.
- **Countersign errors:**
After entering too many invalid passwords on the Countersignature screen, the user who invoked the function requiring the countersignatures will be locked. (For information on countersignatures, see the section **Countersignatures**.)

With the function “List/Unlock Locked Users” you can see which users have been “locked” due to logon or countersign errors. You can also unlock them again.

If the “Lock User Option” is not active, countersign errors are not recorded, whereas logon errors are always recorded (as explained above) regardless of the “Lock User Option”.

How to Invoke Logon/Countersign Errors

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: **Access to Administrator Services** may be restricted (see above).

On the Administrator Services Menu, you select “Logon/countersign errors”. The Logon/Countersign Errors Menu will be displayed, which provides the following functions:

- List error entries
- Delete error entries
- Display individual error entries

■ List/unlock locked users

The individual functions are described below.

When you select one of these functions, you can also specify the following options on the Logon/Countersign Errors Menu:

Order of Records	<ul style="list-style-type: none"> ■ T - The logon error records will be in order of terminal IDs, as defined by the Natural system variable *INIT-ID. For logon errors related to Natural RPC and Natural Web I/O service requests, RPCSRVRQ and NWOSRVRQ respectively will be used instead of the *INIT-ID value. ■ P - The logon error records will be in order of user IDs, as defined by the Natural system variable *INIT-USER. ■ TY - Same as "T" for utility access error records. ■ PY - Same as "P" for utility access error records. <p>This option has no impact on the List/Unlock Locked Users function.</p>
Start Value	<p>If you do not wish to get all, but only a certain range of logon error records or locked users respectively, you may specify a start value as described in the section Finding Your Way In Natural Security.</p> <p>Special start values (for Order of Records = T):</p> <ul style="list-style-type: none"> ■ RPCSRVRQ - for logon errors which occurred in conjunction with Natural RPC service requests. ■ NWOSRVRQ - for logon errors which occurred in conjunction with Natural Web I/O service requests.
Date from/to Time from/to	<p>If you wish to get only records of logon/countersign errors that occurred in a specific period of time, you may specify a period of time in these fields.</p>

List Error Entries

This function displays a list of logon error records.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

To select one error entry from the list to have a closer look at it, you type in the corresponding sequential number (first column of the list) in the "Enter no. to be processed" field. A screen displaying the "Error History" of the selected error will be invoked (this display is the same as for the Display Individual Error Entries function).

Delete Error Entries

This function displays a list of logon error records, similar to that displayed by the List Error Entries function (see above).

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

- If you wish to delete all error entries displayed, press ENTER.
- If you do not wish to delete all error entries displayed, press PF3 to return to the Logon/Counter-sign Errors Menu. If you wish to delete individual error entries, use the Display Individual Error Entries function.

It is recommended that logon error records be deleted periodically so as to save space on the FSEC system file.

See also the direct command ERRDEL below.

Display Individual Error Entries

This function displays the “Error History” of logon error entries one by one.

List/Unlock Locked Users

This function is only applicable if the “**Lock User Option**” (which is described under *General Options* above) is active. It will display a list of those users whose security profiles have been “locked” due to logon or countersign errors. The list will be in alphabetical order of user IDs. On the list you may then unlock individual users.

When you invoke the List/Unlock Locked Users function, the List Locked Users screen will be displayed.

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

The column “T” of the List Locked Users screen indicates the type of error which caused the user to be locked:

C	Countersign error
L	Logon error

In the case of a countersign error, the ID of the owner whose password was entered incorrectly and the ID of the object the locked user attempted to modify will be displayed next to the type.

In the case of a logon error, the error numbers will be displayed next to the type.

To select one entry from the list, you enter the corresponding sequential number (first column of the list) in the “Enter no. to be processed” field. A window will be displayed.

- If you wish to unlock the user, enter a “Y” in the window.
- If you do not wish to unlock the user, leave the “N” already entered in the window unchanged.



Note: You may also unlock a locked user by modifying his/her security profile (as described in the section [User Maintenance](#)).

Deleting All Error Entries - Direct Command ERRDEL

With the [Delete Error Entries](#) function (described above), you can delete logon/countersign error entries page by page.

However, if you wish to delete *all* logon/countersign error entries at once, you enter the direct command ERRDEL in the command line.

Logon Records

Logon records allow you to see which users have been using which libraries.

You can specify the option “Logon recorded” in the security profile of each library and each user (see the sections [Library Maintenance](#) and [User Maintenance](#) respectively).

A logon record will be written by Natural Security:

- every time a user logs on to a library in whose security profile the “Logon recorded” option is set to “Y”;
- every time a user in whose security profile the “Logon recorded” option is set to “Y” logs on to any library.

If the general option “[Transition Period Logon](#)” (see above) is set to “Y”, a logon record will also be written every time an undefined user logs on (regardless of the setting of the option “Logon recorded”), and every time a user logs on to an undefined library.

If the user profile item “ETID” is set to “S” in the “[Library and User Preset Values](#)” (see below), a logon record - with time-stamp-related ETID - will also be written every time a user logs on to Natural (this is only possible if the FUSER system file is not read-only).

Similarly, an access record will be written by Natural Security every time a users invokes a utility in whose default security profile the option “[Access recorded](#)” is set to “Y”.

You may view these logon/access records by using the “Logon records” functions.



Note: Unless explicitly indicated otherwise, the term “logon records” as used in the text below means both logon records and access records

How to Invoke Logon Records

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu, you select “Logon records”. The Logon Records Menu will be displayed, which provides the following functions.

Functions for Logon Records

Each of these functions displays a list of logon records.

Function	Explanation
List Logon Records	With this function, you can view a list of logon records - and have the option to delete individual records.
List Logon Records By Time-Stamp	With this function, you can view a list of logon records in the chronological order of time-stamps (date and time) in which the logons occurred.
Delete Logon Records	With this function, you can view a list of logon records - and have the option to delete whole pages of records.
Delete Logon Records But Last	With this function, you can view a list of logon records - and have the option to delete whole pages of records excepting the latest entry for each user ID (that is, the latest entry for each user ID will not be deleted).

When you select one of the above functions, you can specify the following selection options on the Logon Records Menu:

Order of Records	U	List logon records in alphabetical order of user IDs.
	L	List logon records in alphabetical order of library IDs.
	UX	Same as “U”, but listing only logon records of undefined users.
	LX	Same as “L”, but listing only logon records to undefined libraries.
	Y	List utility access records in alphabetical order of utility names.
	UE	List ETID-related logon records in alphabetical order of user IDs.
	EU	List ETID-related logon records in ascending order of ETIDs.
Start Value	If you do not want a list of all logon records, but would like only certain ones to be listed, you may specify a start value as described in the section Finding Your Way In Natural Security .	

Hex	In this field you can specify a start value in hexadecimal format; for example, for ETID-related logon records.
Date from/to Time from/to	If you wish to view only records of logons which occurred in a specific period of time, you may specify a period of time in these fields. For the function "Delete Logon Records But Last", these fields are ignored.

The Start Value and Date/Time options may be combined.

For the function "List Logon Records By Time-Stamp", only the Date/Time options can be specified, all other selection options are ignored.

Deleting All Logon Records - Direct Command LOGDEL

Considering the amount of space they take up on the FSEC system file, it is recommended to delete logon records at regular intervals.

With the above Delete functions, you can delete logon records page by page.

To selectively delete large numbers of logon records, you can use the application programming interface [NSCADM](#).

If you wish to delete *all* logon records at once, you enter the direct command LOGDEL in the command line.

Maintenance Log Records

This set of functions can only be used if the general option "[Logging of Maintenance Functions](#)" has been activated. If this option has been activated, *log records* are written when security profiles and administrator services settings are modified. The writing of log records allows you to ascertain who has modified which security profiles and administrator services settings. "Modify" in this context comprises all maintenance functions applied to a security profile (including Add, Copy, Delete, Link, etc.); it also includes the transfer of a security profile with the programs SECULD2 and SECLOAD.

To view the log records, you use the "Maintenance log records" functions.

On the Main Menu, you select "Administrator Services". The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu, you select "Maintenance log records". A menu will be displayed, from which you can select the following functions:

- Display Status of Logging Function
- List Administrator Services Maintenance Logs
- List Security Profile Maintenance Logs
- Log File Maintenance
- List Last Logon Records

Display Status of Logging Function

This function displays the following information:

- for which types of objects log records are written,
- the number of log records that have been written for each type of object,
- whether the option “Logging even if no actual modification” is set or not.



Note: For this function, the fields "Object Type", "Start Value" and "Date from/to" on the menu have no effect.

List Administrator Services Maintenance Logs

This function displays a list of the log records that have been written for modifications to administrator services settings.

The log records are listed in chronological order.

On the list, the following information is displayed for each log record: the Administrator Services function performed, the ID of the user who made the modification, and the date and time of the modification.

On the list, you can mark a log record with any character: the screen on which the modification was made will then be displayed; on that screen, fields whose values were changed are displayed intensified. The screen also shows the Natural Security version and FSEC system file with/on which the modification was made.



Note: The version and system-file information is not shown for log records which were written with Natural Security versions prior to 4.2.5. on mainframes and 6.3.5 on non-mainframes.

By default, the "Date from/to" fields on the menu both contain the current date; that is, only the log records written today are listed. To list older log records, you change the date values on the menu as desired before you invoke this function.



Note: For this function, the fields “Object Type” and “Start Value” on the menu have no effect.

List Security Profile Maintenance Logs

This function displays the log records that have been written for modifications to security profiles.

In the "Object type" field, you specify the type of object (User, Library, etc.) whose modified security profiles you wish to be listed. If you leave the field blank or enter a question mark (?), a window will be displayed in which you can select the desired object type. If you enter an asterisk (*), all log records for all security profiles will be listed.

In the "Start value" field, you can enter an object ID as start value for the list to be displayed.

By default, the "Date from/to" fields on the menu both contain the current date; that is, only the log records written today are listed. To list older log records, you change the date values on the menu as desired before you invoke this function.

The log records are listed in chronological order.

On the list, the following information is displayed for each log record: the function performed on the security profile, the ID of the security profile, the ID of the user who made the modification, and the date and time of the modification.

On the list, you can mark a log record with any character: the security profile in which the modification was made will then be displayed. If you press PF2 on the security profile screen, the fields whose values were changed will be displayed intensified (and, if applicable, a message will indicate whether an actual modification was made or not). The screen also shows the Natural Security version and FSEC system file with/on which the modification was made.



Note: The version and system-file information is not shown for log records which were written with Natural Security versions prior to 4.2.5. on mainframes and 6.3.5 on non-mainframes.

Log File Maintenance

On mainframes, this function can only be used in batch mode.

This function allows you to write/read the contents of the log file to/from a work file.

Log records have to be written to a work file when the log file becomes full. Thus, the work file serves as an "archive" for the log records.

The work files to be used are Work File 1 and Work File 5. On UNIX, OpenVMS and Windows, Work File 5 must be a file with the extension ".sag".

The output reports will be written to the print files CMPRT01 and CMPRT02.

When you invoke this function, you will be prompted to specify the database ID and file number of the log file. If you later wish to specify another log file, you press PF5 on the Log File Maintenance menu.

When you invoke this function, the Log File Maintenance menu is displayed, from which you can select the following functions:

Code	Function	Explanation
LI	List Log Records	This function is used to list the contents of the log file. The output contains the same information as displayed by the function List Security Profile Maintenance Logs: a list of all modified profiles/settings, as well as every profile concerned (indicating the profile components which were modified). The output consists of two reports: <ul style="list-style-type: none"> ■ the “List of History Log Entries” report will be written to print file CMPRT01, ■ the “Detail History Log Entries” report will be written to print file CMPRT02.
LX	List Log Records Extended	Same as List Log Records - in addition, this function displays the additional data which are logged if extended logging is activated for user or library profiles; see <i>Extended Logging</i> under Logging of Maintenance Functions .
WR	Write Log Records to Work File	This function is used to write log records from the log file to Work File 5 (without deleting them from the log file).
WD	Write Log Records to Work File and Delete	This function is used to write log records from the log file to Work File 5, and delete them from the log file.
RA	Read Log Records from Work File	This function is used to read log records from Work File 5 onto the log file.
SA	Scan Work File	This function is used to scan the contents of Work File 5.

The Log File Maintenance function can also be invoked with the direct command LOGFILE.

Possible object types to be entered on the Log File Maintenance menu are:

*	all
AD	administration functions
AA	all (base and compound) applications
AB	base applications
AC	compound applications
DD or FI	DDMs/files
LI	libraries
MA	mailboxes
US	users

For object-type codes of external objects, see [Types of External Objects](#).

Other parameters that can be specified on the Log File Maintenance menu are:

Start value	You can specify a start for the objects to be written/read.
Date from/to	If you wish to process only log records that were created in a specific period of time, you may specify a range of dates in these fields.
Work File 1	The name of Work File 1.
Work File 5	The name of Work File 5.

Example:

To write log records from the log file to Work File 5, the CMSYNIN batch input file would contain the following commands:

```
LOGFILE  
FIN
```

The CMOBJIN batch input file might contain the following specifications:

```
SYSSEC,DBA,PASSWORD  
22,241  
WR,US,,2002-07-01,2002-07-25
```

The first line must contain the library ID "SYSSEC" and the user ID and password of the respective Natural Security ADMINISTRATOR.

The second line must contain the database ID and file number of the log file from which the records are read.

The third line must contain the function code and object type (possible values are the same as on the Log File Maintenance menu) - optionally followed by various parameters (whose sequence and possible values correspond to those of the corresponding fields on the Log File Maintenance menu).

When you scan or read the work file, you have to specify the following parameter in the JCL:

```
WORK=((5),OPEN=ACC)
```

Sample Batch Job 1 for Mainframes - Writing Log Records to Work File:

```
//DBA      JOB DBA,CLASS=K,MSGCLASS=X
//**
/*** WRITE LOGGING OF MAINTENANCE DATA TO WORK FILE 5
/*** DELETE RECORDS FROM LOG FILE
/***

//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240)',,
//      'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD  DD DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT DD SYSOUT=X
//CMWKFO5 DD DSN=NSC.LOG.WKF05,
//      DISP=(NEW,CATLG),DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628),
//      SPACE=(TRK,(5,2))
//CMSYNIN DD *
SYSSEC,DBA,password
LOGFILE
22,241
WD,US,,2002-07-01,2002-07-25
.
FIN
/*
/**
```

In the above example, the log records of all user security profiles modified between 1st and 25th July 2002 are written to Work File 5, and are then deleted from the log file.

Sample Batch Job 2 for Mainframes - Writing Log Record Reports to Printers:

```
//DBA      JOB DBA,CLASS=K,MSGCLASS=X
//**
/*** LIST LOG RECORDS-WRITE REPORTS OF MAINTENANCE DATA TO PRINTER
/***

//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240)',,
//      'MT=0,MAXCL=0,MADIO=0,AUTO=OFF')
//STEPLIB DD DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD  DD DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
/*** CMWKFO1 DD DISP=SHR,DSN=NSC.LOG.WKF01
/*** CMWKFO5 DD DISP=SHR,DSN=NSC.LOG.WKF05
//CMPRINT DD SYSOUT=X
//CMPRT01 DD SYSOUT=X
//CMPRT02 DD SYSOUT=X
//CMSYNIN DD *
LOGFILE
FIN
```

```
/*
//CMOBJIN DD *
SYSSEC,DBA,password
22,241
LI,AD,,2002-06-06,2002-06-06
LI,US,MILL*,2002-05-01,2002-05-31
.
/*
//*
```

In the above example, the log records of all administrator services settings modified on 6th June 2002 and of all user security profiles modified in May 2002 are written to print files CMPRT01 (list of log records) and CMPRT02 (detailed log records information).

Sample Batch Job 3 for Mainframes - Reading Log Records from Work File:

```
//DBA          JOB DBA,CLASS=K,MSGCLASS=X
//**
//** READ LOGGING OF MAINTENANCE DATA FROM WORK FILE 5
//** INTO LOG FILE
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D, FNAT=(22,210), INTENS=1, FSEC=(22,240), ',
//      'MT=0, MAXCL=0, MADIO=0, AUTO=OFF, WORK=((5), OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD, DISP=SHR
//DDCARD  DD   DISP=SHR, DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT DD   SYSOUT=X
//CMWKF05 DD   DSN=NSC.LOG.WKF05, DISP=(SHR)
//CMSYNIN  DD *
SYSSEC,DBA,password
LOGFILE
22,241
RA,US,,2002-07-01,2002-07-25
.
FIN
/*
//*
```

In the above example, the log records of all user security profiles modified between 1st and 25th of July 2002 are read from Work File 5 and thus restored on the log file.

See also the section [Natural Security In Batch Mode](#).

List Last Logon Records



Note: This function is independent of the logging of maintenance functions. Internally, however, it uses the same log file.

This function evaluates the logon records that have been written by Natural Security (see [Functions for Logon Records](#) above). It allows you to ascertain:

- when each user logged on last,
- which users have not logged on within the last n days.

When you invoke the function, a window will be displayed in which you enter a number of days :

- If you enter a "0", you will get a list of logon records showing the latest logon record written for each user.
- If you enter any other value n , you will get a list of logon records of those users who have not logged on in the last n days, showing for each of those users the last logon record written before the specified time interval.

The logon records are listed in chronological order.



Note: For this function, the fields "Object Type", "Start Value" and "Date from/to" on the menu have no effect.

SAF Online Services

SAF Online Services provide several functions for monitoring the SAF server.

SAF Online Services are only available on mainframe computers; they are only available if Natural SAF Security (or any other SAF-related Software AG product) is installed.

Before you can use SAF Online Services, you have to define a utility security profile for the utility SYSSAFOS (which contains the SAF Online Services).

To invoke SAF Online Services, you select "Administrator Services" on the Main Menu. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu, you select "SAF online services". The Online Services menu will be displayed, which provides the following functions:

- [System Parameters](#)

- [System Statistics](#)
- [User Statistics](#)
- [Zap Maintenance](#)
- [Storage Display](#)
- [System Tracing](#)
- [Refresh Server](#)

System Parameters

This function displays the parameter settings as defined in the system parameter module. The following information is displayed:

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server that are related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Class/Type	Shows the names of the different SAF general resources Classes or Types. These contain either the default or any override values which have been defined in the system parameter module.
Universal	This indicates a particular check is designated universal. If selected, then failure to define a particular resource profile will result in all users having access to it. Natural Program execution authorization cannot be designated universal.
Buffered	Displays for each type of check the maximum number of positive checks that the SAF server can buffer on behalf of each user.
Logging	This indicates the SMF logging level required when performing security checks. "0" signifies logging ASIS, that is, in accordance with the default for the security Class/Type; "1" indicates an override setting of NONE.
Active	Designates the particular authorization checks that are active. This applies only to checks performed by mainframe Natural as all other checks are activated by the installation process.
Env (Environment)	Indicates that an environment code, based on the Natural system files, is used to prefix certain resource profiles. Applies only to authorization checks performed by mainframe Natural.
Storage (k)	The size of the buffer in kilobytes which can be used for caching positive security checks in the address space of the SAF server.
Server DBID	Shows the database ID used by the SAF server.
Encrypt Req.	Indicates whether security requests passed between different SAF server components are communicated encrypted.
Encrypt Stg.	Indicates whether storage maintained within the Natural environment is kept in an encrypted state.
Messages	SAF server message level: Level "0" gives only error message, "1" reports security violations and "3" generates an audit trail of all checks.
Cmd Log	Indicates whether command logging is turned on.

Item	Explanation
Buffer	Indicates whether security checks will be cached by the SAF server.
JCL check	Indicates whether CA-JCL check processing is available within the Natural environment.
Prefix Prog	Indicates whether Natural program names are prefixed with the name of the current application library when performing authorization checks. <i>Not applicable to Natural SAF Security.</i>
Protect Obj	Indicates whether program objects are protected within the Natural environment. Users require ALTER access to a particular application in order to modify its program objects. <i>Not applicable to Natural SAF Security.</i>
Log SYSMAIN	Indicates whether logging of all SYSMAIN operation is required. <i>Not applicable to Natural SAF Security.</i>
SYSMAIN/Lib	Indicates whether authorization checks for SYSMAIN functions will include access to the relevant Natural application libraries. <i>Not applicable to Natural SAF Security.</i>
Cmd Line	Indicates whether the Natural command line is protected. Users require CONTROL access in order to enter commands in the Natural command line.
ETID	Indicates whether Natural will generate a unique ETID.
Edit/Lib	Indicates whether Natural will prevent editing of objects located in another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Clear/Ed	Indicates whether Natural will clear the edit area when logging onto another Natural application library. <i>Not applicable to Natural SAF Security.</i>
Ext Name	Indicates whether Natural will take the user name from SAF. Specifically, the field *USER-NAME will be taken from RACF or CA-ACF2.
Ext Group	Indicates whether Natural will take the group name from SAF. That is, the field *GROUP will be taken from RACF, CA Top Secret, CA-ACF2.
Log API	Indicates whether SMF logging is performed when executing the Natural API.
Env API	Indicates whether authorization checks performed by the Natural API will be prefixed by an environment code based on the Natural system files.

System Statistics

This function displays statistical information on the SAF server. The following information is displayed:

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Check (+ve)	Indicates the number of authorization checks performed against the security system for each check type. The count indicates authorizations for which access was permitted and can include universal checks.
Check (-ve)	Indicates the number of authorization checks performed against the security system for which access was denied.

Item	Explanation
Check saved	Shows the number of authorization checks that were optimized by the SAF server because the result was already known.
Overwritten	Number of times positive authorization results were overwritten in the SAF server's cache because more recent information took its place in the buffer. Increase the number of items buffered if this count is excessive for any particular check type.
Lngh	Number of bytes reserved to cache resource profiles belonging to each type of authorization check. This value is generated automatically by the system.
Active Users	Number of users currently active in the SAF server.
High Watermark	High watermark value for number of users present in the SAF server.
Max Users	Maximum of users that can be accommodated.
Overwritten	Number of times a user area was reclaimed and allocated to another user. Increase the total buffer size if this count becomes excessive.
Authenticated	The total number of successful authentication checks performed.
Denied	The number of unsuccessful authentication checks.

User Statistics

This function displays statistical information on the currently active users. The function displays a list of users. When you select a user from the list, statistical information on this user will be displayed. The individual items correspond to those of the same names as described above for System Statistics.

Zap Maintenance

This function displays a list of ZAPs applied to the SAF server.

Storage Display

This function displays the storage of the SAF server's address space.

System Tracing

This function displays a list of the 256 most recent trace events.

Refresh Server

This function is used to restart the SAF server.

It ensures that all data held in the SAF server's own buffer are flushed, including the settings of NSF Options, the [System Statistics](#), cached security checks and user information. In addition, any data held by the security system itself in the address space of the SAF server are flushed when this function is executed.

User Default Profiles

Before you use default profiles, you should be familiar with the “normal” way of defining users as explained in the section [User Maintenance](#).

When you add new users, you can either type in every item of every user security profile by hand, or you can use a pre-defined user default profile as a template for the creation of a user security profile. When you have to define numerous users whose security profiles are to be very similar to one another, you can define in a default profile the items which are to be the same for many users, and then use this default profile as the basis for the individual security profiles. By using default profiles, you can thus reduce the amount of work required to define users to Natural Security.

You create a default profile as described below, and then use it as a template for a user security profile as described in the section [User Maintenance](#).

How to Create a Default Profile

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu 2, you select “User default profiles”. The Default User Profiles selection list will be displayed.

In the command line of this screen, enter the command “ADD”. The Add User Default Profile window will be displayed.

In this window, enter the following:

- the *user ID* of the default profile,
- the *user type* of the default profile.

For information on user IDs and user types, see the section [User Maintenance](#).

The Add User Default Profile screen will be displayed. On this screen you define a user default profile.

The Add User Default Profile screen corresponds more or less to the Add User screen for the same user type. The individual items you may define as part of a user profile are described under *Components of a User Profile* in the section *User Maintenance*. However, please note that you can define some items only in an individual security profile, but not in a default profile.

Default profiles are maintained like individual user profiles (as described in the section *User Maintenance*).

How to Use a Default Profile

When you add a new user, you can specify the ID of a default profile which is to be used as a template for the user security profile you are creating.

The *user type* of the default profile must be the same as that of the security profile you use it for.

When you use a default profile to add a new user, the items from the default profile are copied into the user profile - except the user ID, user name and the owners.

In the user profile, you can overwrite the items copied from the default profile, and specify further items.



Note: To define numerous users who are to have identical security profiles, you can also use the **“Multiple Add User”** function (which is described in the section *User Maintenance*).

Library Default Profiles

Before you use default library security profiles, you should be familiar with the “normal” way of defining libraries as explained in the section *Library Maintenance*.

When you add new libraries, you can either type in every item of every library security profile by hand, or you can use a pre-defined default library profile as a template for the creation of a library security profile. When you have to define numerous libraries whose security profiles are to be very similar to one another, you can define in a default profile the items which are to be the same for many libraries, and then use this default profile as the basis for the individual security profiles. By using default library profiles, you can thus reduce the amount of work required to define libraries to Natural Security.

You create a default profile as described below, and then use it as a template for a library security profile as described in the section *Library Maintenance*.

How to Create a Default Profile

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

On the Administrator Services Menu 2, you select “Library default profiles”. The Default Library Profiles selection list will be displayed.

In the command line of this screen, enter the command `ADD`. The Add Default Library Profile window will be displayed.

In this window, enter the `library ID` of the default profile (for information on [library IDs](#), see the section *Library Maintenance*).

The Add Default Library Profile screen will be displayed. On this screen, you define a default library profile.

The Add Default Library Profile screen corresponds more or less to the Add Library screen. The individual items you may define as part of a library profile are described under [Components of a Library Profile](#) in the section *Library Maintenance*. However, please note that you can define some items only in an individual security profile, but not in a default profile.

Default profiles are maintained like individual library profiles (as described in the section [Library Maintenance](#)).

How to Use a Default Profile

When you add a new library, you can specify the ID of a default profile which is to be used as a template for the library security profile you are creating.

When you use a default profile to add a new library, the items from the default profile are copied into the library profile - except the library ID, library name and the owners.

In the library profile, you can overwrite the items copied from the default profile, and specify further items.

Library and User Preset Values

Before you start defining users and libraries to Natural Security, you can use this function to pre-define the values of several items that are part of a library profile and user profile. When you then create a library security profile or user security profile, the items in the profile you are creating are already pre-set to these values.

► To invoke this function:

- 1 Select "Administrator Services" on the Main Menu. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

- 2 On the Administrator Services Menu 2, you select "Library and user preset values".

The first Preset Values screen will be displayed, containing [library profile items](#). A second screen contains [user profile items](#). With PF7 and PF8 you can switch between the two screens.

With PF5 on the library profile items screen, you can invoke another screen with [further library options](#).

The items are explained below.

Library Profile Items

Some of these items also appear in the security profile of every library, where their values will be preset to those you specify on the Preset Library Values screen. If the general option "[Overwriting of defaults possible](#)" (see above) is set to "Y", you may overwrite these values in the individual library security profiles. Other items do not directly correspond to library profile fields, but are options which apply to library profiles in general.

Item	Explanation
Active cross-reference for Predict	Determines whether an active cross-reference in Predict is generated for a library. If you specify an asterisk (*) here, this applies to all libraries: The generation of active cross-references will be determined by the value of the Natural profile parameter XREF, regardless of the "Cross-reference" setting in individual library profiles.
Logon recorded	Determines whether logons to a library are recorded.

Item	Explanation		
Natural programming mode	<p>Determines whether the programming mode can be changed with the Natural profile/session parameter SM.</p> <p>If you specify an asterisk (*) here, this applies to all libraries: The programming mode will be determined by the value of the Natural profile parameter SM, regardless of the "Programming mode" setting in individual library profiles.</p>		
Restart	Determines whether an Adabas OPEN command with or without End of Transaction ID (ETID) is executed during the logon procedure.		
Maintenance with Natural utilities	Determines who may maintain the contents of the library with Natural utilities.		
Clear source area by logon	Determines whether the editor's source work area is cleared automatically when a user logs on from the library to another library.		
Execute startup transaction in batch	Determines whether the startup transaction specified in the library profile is executed in batch mode.		
Steplibs	<p>Allows you to specify the libraries which are to be the steplib libraries for the library.</p> <p>You can specify the name of the first steplib in the Steplibs field on the Preset Library And User Values screen. To specify more than one steplib, enter an asterisk (*) in the field or press PF4: a window will be displayed, in which you can specify up to 9 steplibs.</p>		
Profile parameters for undefined libraries	<p>This is an option which applies to undefined libraries in general.</p> <p>For libraries for which no security profiles have been defined yet, the following settings will be determined by the corresponding Natural profile parameters:</p> <table border="1"> <tr> <td>NC</td><td>Allow system commands.</td></tr> </table>	NC	Allow system commands.
NC	Allow system commands.		
RPC Server Session Options (Natural RPC Restrictions)			
Close all databases	Controls the logon-/logoff-dependent closing of databases opened by remote subprograms in a library.		
Logon option	Determines which logon data are evaluated when a library is accessed via a Natural RPC service call.		
Logon recorded	This is not only a preset value. It also applies as default value if the corresponding field in the library profile is set to "*". If this is the case, it determines whether access to a library is to be recorded or not when the library is accessed via a Natural RPC service call.		

Item	Explanation
Lock user option	This is not only a preset value. It also applies as default value if the Lock User option in the security profile of the Natural RPC server is set to "*". If this is the case, it controls the locking of users when they attempt to access a library on that server via a Natural RPC service call:
	N No locking of users will be performed.
	X Once a user has reached the maximum number of logon attempts without supplying the correct password, he/she will be locked, that is, the user ID will be made "invalid". Natural Security "remembers" unsuccessful attempts across sessions: The error counters for the client user IDs which were tried out unsuccessfully are kept for access attempts in subsequent sessions, thus reducing the number of subsequent attempts with these IDs. The error counter for a user ID is only reset after a successful logon.
	* The locking of users is controlled by the Lock User Option in the General Options section of Administrator Services.
For details on this feature, see also the Lock User Option under <i>General Options</i> .	

Further Library Options

- **Module Protection Mode**
- **Disable Rename and Delete of Library Node**
- **NDV Startup Inactive**

Module Protection Mode

This option applies to all libraries. It affects the way in which the **Disallow/Allow Modules** settings in library security profiles are evaluated.

*	<p>The evaluation of the Disallowed/Allowed settings depends on the platform:</p> <ul style="list-style-type: none"> ■ On mainframe computers: When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is only evaluated if the module is contained in that library. ■ On other platforms: When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is <i>always</i> evaluated, regardless of whether the module is contained in the current library or another library (steplib).
---	---

L	<p>The evaluation of the Disallowed/Allowed setting is the same on any platform:</p> <p>When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is only evaluated if the module is contained in that library.</p> <p>Setting this option to "L" may be useful if you transfer a Natural application from a mainframe to a non-mainframe platform and wish to keep you module protection unchanged.</p>
---	---

Disable Rename and Delete of Library Node

This option can be used to prevent the inadvertent deletion/renaming of a library in the mapped environment of the Natural Development Server. It applies to the actions Rename and Delete in the context menu of the library node in the mapped environment (see [Tree-View Actions](#) in the section *Protecting the Natural Development Server Environment and Applications*).

Y	The actions Rename and Delete are disabled. They cannot be selected from the context menu of the library node.
N	The actions Rename and Delete are available in the context menu of the library node.



Note: Setting this option to "Y" cannot prevent that a library disappears from the tree view if the objects it contains are deleted (either from within the library or with utilities from outside the library).

NDV Startup Inactive

This option can be used to suppress the execution of [startup transactions](#) for logons to libraries in a mapped environment on a Natural Development Server client (see also *Map Environment and Library Selection* in the section *Protecting the Natural Development Server Environment and Applications*).

Y	Startup transactions are not executed in a mapped environment. The name of the startup transaction, as specified in the security profile of the library to which a logon is performed, is not written into the Natural system variable *STARTUP.
N	The execution of startup transactions in a mapped environment is not restricted.

This option only takes effect in mapped environments on Natural Development Server clients.

User Profile Items

Some of these items also appear in the security profile of every user, where their values will be preset to those you specify on the Preset Library And User Values screen. If the general option "[Overwriting of defaults possible](#)" (see above) is set to "Y", you may overwrite these values in the individual user security profiles. Other items do not directly correspond to user profile fields, but are options which apply to user profiles in general.

Item	Explanation
ETID	<p>You may specify which value is to be used as ID for End of Transaction data (ETID).</p> <p>For Natural Security to be able to supply ETIDs, the Natural session must be started with the Natural profile parameter ETID being set to "OFF" or its default value.</p>
	<p>S</p> <p>This setting applies to all users; it cannot be changed in individual user profiles.</p> <p>An ETID for every user will be generated by Natural Security at the start of the his/her Natural sessions. Such an ETID consists of "S", followed by a time-stamp (the leftmost 7 bytes of the value of the Natural system variable *TIMESTAMP at session start), and uniquely identify the user session. It will remain in effect until the user ends his/her Natural session.</p> <p>In the individual user profiles, this is indicated by the Default ETID field being prefixed with "S>"; any not time-stamp-related ETID value shown in that field will then not be used.</p> <p>To use a time-stamp-related ETID for a single user only, you specify *TIMESTAMP in the Default ETID field of the individual user profile.</p> <p>If time-stamp-related ETIDs are used, a logon record containing the ETID will be written by Natural Security every time a user logs on to Natural. To ascertain which ETID has been used by which user ID, you can view the logon records, or use the application programming interface NSCADM.</p> <p>For service requests in an RPC client/server environment, you can also use time-stamp-related ETIDs; see Components of an RPC Server Profile.</p> <p>Note: With ETID=S, the Natural system variable *ETID contains binary, non-printable data; this may affect your applications if they evaluate the *ETID value. For the display, you may consider using an edit mask; e.g. EM=(H(8)).</p>
	<p>G</p> <p>ETIDs will be generated by Natural Security during the logon procedure from the following components:</p>

Item	Explanation
	<ul style="list-style-type: none"> ■ The 1st byte is single character that identifies the environment from which Natural is invoked (B=Batch, C=Color, P=PC, T=TTY, V=Video, X=BTX). ■ The 2nd to 5th bytes is a unique string of alphanumeric characters that identifies the user (this string is generated when a user is defined to Natural Security). Only these 4 bytes are displayed in the user's security profile. ■ The 6th to 8th byte is a unique string of alphanumeric characters that identifies the library (this string is generated when a library is defined to Natural Security).
	<p>U</p> <p>The ID by which a user is defined to Natural Security, i.e. the value of the Natural system variable *USER, will be used as ETID.</p> <p>If the Automatic Logon feature (which is described in the section <i>Logging On</i>) is used, the value of *USER will be identical to that of *INIT-USER.</p>
	<p>I</p> <p>The value of the Natural system variable *INIT-USER will be used as ETID.</p>
	<p>T</p> <p>The value of the Natural system variable *INIT-ID will be used as ETID.</p>
	<p>N</p> <p>ETIDs will not be used.</p> <p>If you do not remember the possible values you may specify, enter a question mark (?) or an asterisk (*) in the field: a window will be displayed; in the window, mark the desired value with a character or with the cursor; the value will then be written into the ETID field.</p> <p>See the <i>Natural System Variables</i> documentation for details on the above-mentioned system variables.</p>
Private library for administrator/person	Determines whether the user, if he/she is of type PERSON or ADMINISTRATOR, may have a personal ("private") library.
Message before password expiration	<p>This option applies to user profiles in general. You can use it to have a message displayed to users whose password is about to expire.</p> <p>The number you specify here - possible values are 1 to 10 - determines how many days before his/her password expiration is due a user is to receive a message, indicating that his/her password will expire. The message (NAT1691) will be displayed after the initial logon to Natural.</p> <p>This only applies to users in whose security profiles a time interval for password change is set (option "Change after <i>nnn</i> days" in a user profile.)</p>
Minimum password length	<p>This option applies to user profiles in general.</p> <p>A user password must not consist of fewer characters than the number specified here. Possible values are 1 to 8.</p>

Item	Explanation				
	When you set this length, please bear in mind that by default passwords are identical to user IDs (see the section User Maintenance).				
Password case-sensitive	<p>This option applies to user profiles in general. It determines whether or not Natural Security is to distinguish between lower-case and upper-case characters in user passwords:</p> <table> <tr> <td>N</td><td>Natural Security internally converts all alphabetical characters in passwords to upper-case.</td></tr> <tr> <td>Y</td><td>Natural Security distinguishes between lower-case and upper-case characters in passwords.</td></tr> </table> <p>See also Password Rules below.</p> <p>Note: If you set this option to “Y”, make sure that any password input fields used also distinguish between lower-case and upper-case. This may affect the logon screen, the user exit LOGONEX1, any logon-related Natural Security application programming interfaces, or Natural's RPC-logon-related application programming interfaces.</p>	N	Natural Security internally converts all alphabetical characters in passwords to upper-case.	Y	Natural Security distinguishes between lower-case and upper-case characters in passwords.
N	Natural Security internally converts all alphabetical characters in passwords to upper-case.				
Y	Natural Security distinguishes between lower-case and upper-case characters in passwords.				
User password history	This field corresponds to the general option User Password History .				

Password Rules

The following options can only be used if the general option [User Password History](#) is active. They allow you to define rules to which user passwords must conform:

Maximum number of stored passwords	<p>This corresponds to the field in the User Password History activation window:</p> <p>The last <i>nn</i> passwords used by each user are recorded by Natural Security. These last <i>nn</i> passwords cannot be used again by the user as new password. Possible values: 1 - 99.</p>
---	--

Password mask	You can define a "mask" to which passwords must conform; that is, you can define for each position in a password what it has to consist of:	
	A	In this position, an alphabetical character (if "Password case-sensitive" is set to "N") or an upper-case alphabetical character (if "Password case-sensitive" is set to "Y") has to be specified.
	a	In this position, a lower-case alphabetical character must be specified (this only possible if "Password case-sensitive" is set to "Y").
	N	In this position, a number must be specified.
	E	In this position, a special character (that is, neither an alphabetical character nor a number) must be specified.
	*	In this position, any character can be specified.
	For example, "***NNN" means that the first three characters can be any characters, while the second three have to be numbers. The length of the mask must correspond to the Minimum Password Length (see above).	
Each character only once	If this value is set to "Y", passwords must not contain a character twice. For example, "THIRST" would not be allowed, because it contains two T's.	
Disallow double characters	If this value is set to "Y", passwords must not contain double characters. For example, "LITTLE" would not be allowed, because of the double T.	
Check password for pattern	If this value is set to "Y", a password must not be the same as the current value of the Natural system variable *USER. Moreover, a new password must not be too similar to the old one: a new password will be rejected if its last three characters are identical to those of the old password.	
The following options are only available if "Password case-sensitive" (see above) is set to "Y". The sum of these three values must correspond to the "Minimum Password Length" (see above):		
Minimum no. of upper-case letters	In this field, you can specify how many upper-case alphabetical characters passwords must contain at least.	
Minimum no. of lower-case letters	In this field, you can specify how many lower-case alphabetical characters passwords must contain at least.	
Minimum no. of non-letters	In this field, you can specify how many non-alphabetical characters passwords must contain at least.	



Note: To ascertain in which user security profiles the value of a specific component differs from the corresponding preset value, you can use the application programming interface **NSCADM**.

Definition of System Libraries

This function is used as part of the installation procedure for an initial installation of Natural Security. It allows you to automatically create library security profiles for system libraries (that is, libraries whose names begin with "SYS") of Natural and its subproducts.

If you use this function, you have to set the Natural profile parameter MADIO to a value of at least "2000".

You should not apply this function to SYS libraries containing Natural utilities, as it is recommended that utilities be protected as described in the section [Protecting Utilities](#).

► To define system libraries:

- 1 On the Main Menu, you select "Administrator Services".

The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

- 2 On the Administrator Services Menu 2, you select "Definition of system libraries".

A list of the system libraries of Natural and all Natural subproducts installed at your site will be displayed. For each system library, a library-specific security profile is provided in which all the necessary components are already defined appropriately.

- 3 On the list, you can either mark with "AD" individual libraries to which you wish their pre-defined profiles to be applied one by one, or you can choose to have the pre-defined profiles applied to all product system libraries simultaneously by marking the corresponding product with "AD".

For further information, see the Natural Security installation description in the Natural *Installation* documentation.

Definition of Undefined Libraries

This function is used to create library security profiles for undefined libraries, that is, libraries which exist on the current FUSER system file, but for which no library security profiles have been created.

This function corresponds to that provided by the SHOW command, as described under [Listing Undefined Libraries](#) in the section *Library Maintenance*.

▶ **To define undefined libraries:**

- 1 On the Main Menu, you select "Administrator Services".

The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (see above).

- 2 On the Administrator Services Menu 2, you select "Definition of undefined libraries".

A list of all undefined will be displayed. It corresponds to the one you get when you issue the command SHOW UNDF on the Library Maintenance selection list.

- 3 Proceed as described under [Listing Undefined Libraries](#) in the section *Library Maintenance*.

7

User Maintenance

■ Before You Begin	96
■ Components of a User Profile	96
■ Creating and Maintaining User Profiles	105

This section describes how to create and maintain *user security profiles*. It covers the following topics:

Before You Begin

Before you begin to define users to Natural Security, it is recommended that you take a few preparatory steps:

- Make a list of all people in your organization who are using Natural.
- Divide them into groups according to the work they do and in view of the Natural libraries they are to use. The division of your company into departments may be a guideline. People using the same libraries should be in the same groups. (People may be in more than one group.)

It is recommended that groups be used as much as possible, as this will not only reduce Natural Security maintenance considerably, but also provides for a more consistent protection setup.

The definition of users to Natural Security and the assignment of users to groups is best done in the following order:

1. Create a group security profile; that is, define a user of type GROUP.
2. Create individual user security profiles; that is, define users (typically of type MEMBER).
3. Assign MEMBERS to the GROUP; that is, modify the GROUP security profile.

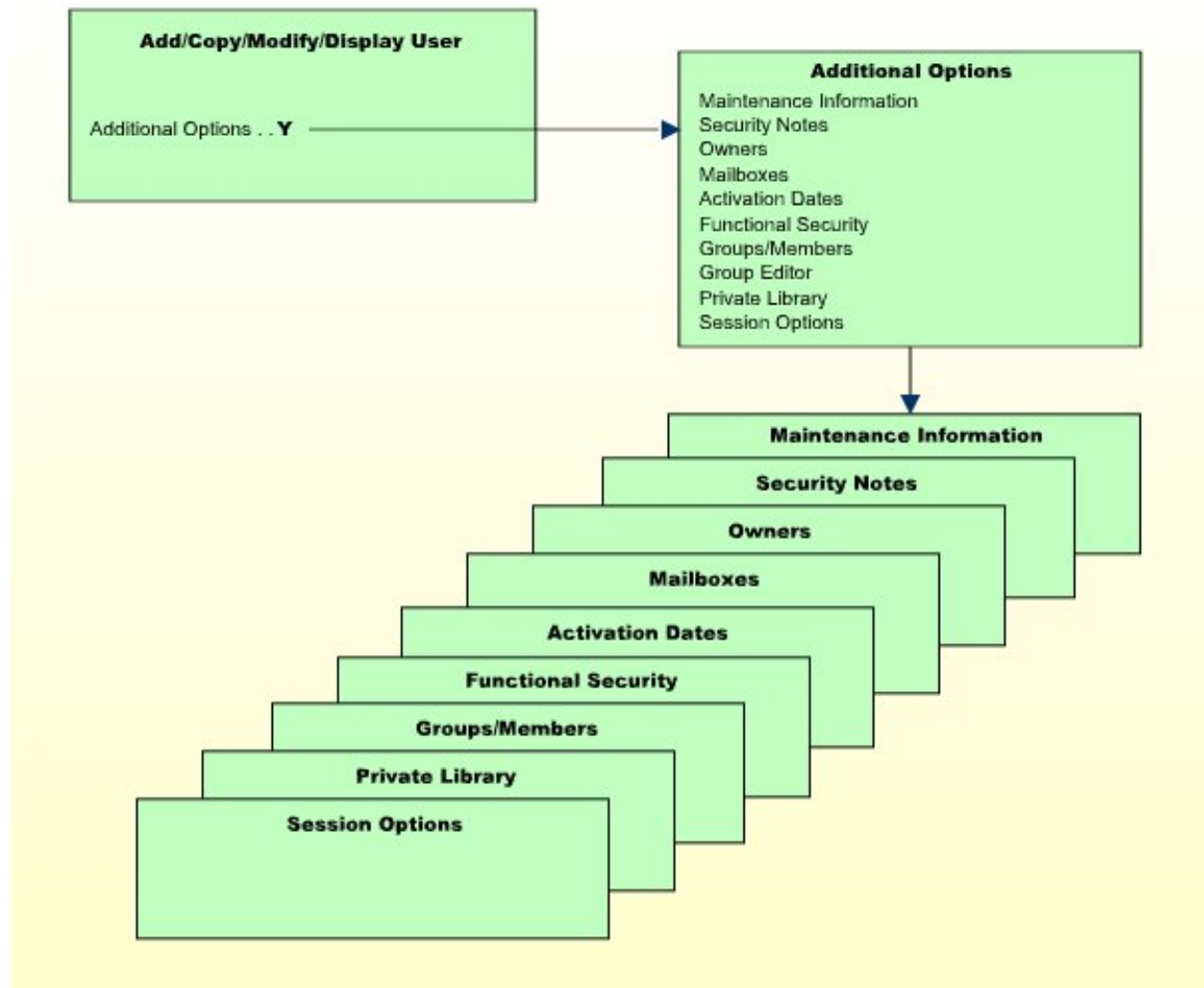
Components of a User Profile

This section covers the following topics:

- [Overview of Components](#)
- [Components on Main User-Profile Screen](#)

- Additional Options

Overview of Components



Components on Main User-Profile Screen

The following type of screen is the "basic" user profile screen, which appears when you invoke one of the functions Add, Copy, Modify, Display for a user security profile:

15:27:08

*** NATURAL SECURITY ***
- Modify User -

2009-01-18

Modified ..

by

User ID AD

User Name ARTHUR DENT_____

User Type A (A=Administrator, P=Person, M=Member)

Privil. Groups

DOC_____

No. groups 3

Libraries

Default .. SYSSEC__

Last

ETID

Default .. AR1R G

Last

Password

New Password _____

Change after 666 days

Batch User ID _____

Language 0

Private Library ... N

Logon recorded N

Additional Options ... N

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---

Help PrevM Exit AddOp PrLib Flip

Canc

The individual items you may define as part of a user security profile are explained below.

The items of a user security profile may vary depending on the user type. For each item explained below, the user types concerned are indicated in brackets. If no user types are indicated, the item applies to users of every type.

Field	Explanation
User ID (display only)	The ID of the user as specified when the user security profile was created.
User Name	The name of the user, which may be up to 32 characters long. This name should be identical to the corresponding entry in Predict (if installed).
User Type	G = Group M = Member A = Administrator P = Person,

Field	Explanation
	<p>T = Terminal B = Batch User</p>
Privileged Groups (A, P, M, T, B)	<p>You may enter the IDs of up to five groups to which the user belongs. By this, you may influence the order in which Natural Security scans for a link to a library:</p> <ul style="list-style-type: none"> ■ For users of type MEMBER the following applies: When the user tries to log on to a protected library, the privileged groups entered in his/her security profile are checked (in order of entry) for a link to the library before the other groups to which the user belongs are checked (in alphabetical order) for a link to the library. ■ For users of type ADMINISTRATOR and PERSON the following applies: When the user tries to log on to a protected library to which he or she is not linked directly, the privileged groups entered in his/her security profile are checked (in order of entry) for a link to the library before the other groups to which the user belongs are checked (in alphabetical order) for a link to the library. ■ For TERMINALS, the following applies: When a user tries to log on to a protected library by means of the terminal ID (that is, without entering a user ID), the privileged groups in the terminal's security profile are checked (in order of entry) for a link to the library before the other groups to which the terminal belongs are checked (in alphabetical order) for a link to the library. <p>The privileged groups may also be used to influence the order in which Natural Security searches for utility profiles to apply; see Which Utility Profile Applies? in the section <i>Protecting Utilities</i> for details.</p> <p>You may enter a group in the Privileged Groups list only after the user has been added to the group.</p> <p>If you remove a group from the user's Privileged Groups list, the user will <i>not</i> be deleted as a member of that group.</p>
Members (G)	<p>You may enter the IDs of the first five users to belong to this group. If the number of users belonging to the group exceeds five, use the Edit Group Members functions (see Editing Group Members below).</p> <p>You can assign users to a group only after they have been defined to Natural Security.</p>
No. of Groups (A, P, M, T, B; display only)	<p>The total number of groups to which the user belongs (including the Privileged Groups). By means of the "Additional Options" (see below), you can obtain a list of all these groups.</p>
No. of Members (G; display only)	<p>The total number of users which belong to the group. By means of the "Additional Options" (see below), you can obtain a list of all these users.</p>
Default Library	<p>In this field, you may enter the ID of a default library.</p> <ul style="list-style-type: none"> ■ For users of type ADMINISTRATOR, PERSON, or MEMBER the following applies: The default library specified in a user's security profile will be invoked automatically when the user logs on to Natural without entering a library ID.

Field	Explanation
	<ul style="list-style-type: none"> ■ For TERMINALs, the following applies: The default library specified in a terminal's security profile will be invoked automatically when a user logs on to Natural by means of the terminal without entering a library ID. ■ For GROUPs, the following applies: The library specified in a group's security profile will be invoked automatically when a user logs on to Natural without entering a library ID if the user has no default library specified in his/her own security profile, and if the group is among the privileged groups listed in the user's security profile.
Last Library (A, P, M, T, B; display only)	The last RESTARTable library to which the user was logged on. (The Restart option in a library profile determines whether a library can be RESTARTed.)
Default ETID (A, P, M, T, B)	<p>This field displays the ID to identify End of Transaction data (ETID).</p> <ul style="list-style-type: none"> ■ If this field is prefixed with "S>", this indicates that time-stamp-related ETIDs for all users are generated by Natural Security at session start. In this case, the actual ETID value shown in the user profile will not be used. See ETID=S under Library and User Preset Values in the section <i>Administrator Services</i> for details. ■ If the ETID displayed is followed by a "G", this indicates that it has been generated by Natural Security as described for ETID=G under Library and User Preset Values. If it has not been generated and you wish it to be generated, enter a "?" in the Default ETID field. ■ Other possible ETID values (user ID, TP user ID or terminal ID) are described under Library and User Preset Values. <p>Note: ETIDs can only be supplied by Natural Security if the Natural session is started with the Natural profile parameter ETID being set to "OFF" or its default value.</p>
Last ETID (A, P, M, T, B; display only)	The ETID which was last generated/set for the user.
New Password (A, P, M)	<p>You may enter a password for the user to be used when he or she logs on.</p> <p>This password may be modified by the user (during the logon procedure) or by an owner of the user's security profile (in the security profile).</p> <p>If no password is entered here, Natural Security will assume the password to be identical to the user ID.</p> <p>The minimum length of the password is set in the Library and User Preset Values section of Administrator Services.</p>
Change after <i>nnn</i> days (A, P, M)	<p>In this field, you may specify a time interval after which the user will be forced to change his or her password during the logon procedure.</p> <p>For example, if you set the time interval to "007", the user has to enter a new password on the logon screen every 7 days. If the user fails to do so, he or she cannot log on.</p>

Field	Explanation
	If you wish to prevent the user from changing the password, set this field to "999"; the user will then not be able to change his/her password at the login.
Batch User ID (A, P, M, G)	<p>If the Natural system variable *DEVICE is set to "BATCH", the following applies:</p> <p>You may enter the ID of a batch user profile. Before you can enter a batch user ID, a security profile for this batch user ID must have been defined.</p> <p>In batch mode, a user logs on with his/her "normal" user ID and password. Natural Security will then use the batch user ID specified in the user's security profile, and the conditions of use defined for that batch user ID will apply.</p> <p>If no batch user ID is specified in the user's security profile, the "Privileged Groups" specified in the user's security profile will be checked (in order of entry) for a batch user ID. If none of the Privileged Groups has a batch user ID either, the user's own user ID will be used.</p> <p>Note: This option only applies if the Natural system variable *DEVICE is set to "BATCH"; otherwise, this option has no effect.</p>
Language (A, P, M, G, B)	<p>This corresponds to the Natural system variable *LANGUAGE and controls the usage of Natural error messages.</p> <p>You may enter a numeric value from 1 to 60. Each value represents one language (for example, "1" stands for "English"). If you set the value to "0", the value of the Natural profile parameter ULANG applies.</p> <p>For further information, see the system variable *LANGUAGE and the profile parameter ULANG (in the <i>Natural System Variables and Parameter Reference</i> documentation respectively).</p>
Time Differential (T, G)	<p>This only applies to an environment in which remote nodes are used in a computer network. It corresponds to the Natural profile parameter TD (which is described in the <i>Natural Parameter Reference</i> documentation).</p> <p>You may enter a value from "-23" to "+23" for hours, and "00" or "30" for minutes. The values indicate the number of hours/minutes added to/subtracted from computer centre time to obtain local time. The default value is "0" (which means that computer centre time will be used).</p> <p>If, for example, your location time is 5 hours ahead of computer centre time, you may set the value to "+5" if you wish to use actual local time instead of computer centre time.</p> <p>You can also specify an asterisk (*); this has the same effect as the profile parameter setting TD=AUTO (that is, the time differential will be computed automatically by comparison of physical and logical machine times).</p> <p>You can use either Time Differential or Time Zone (described below), but not both.</p>
Time Zone (T, G)	This only applies to an environment in which remote nodes are used in a computer network.

Field	Explanation
	<p>You may enter the name of a time zone. A time zone of this name must be defined in the NTTZ macro of the Natural configuration module NATCONFIG. The definition in the NTTZ macro determines the number of hours/minutes added to/subtracted from computer centre time to obtain local time.</p> <p>You can use either Time Zone or Time Differential (described above), but not both.</p>
Private Library (A, P)	This option determines whether the user may have a private library (see below).
Logon recorded	<p>All logons by the user to any library will be recorded.</p> <p>See Logon Records in the section <i>Administrator Services</i> for information on logon records.</p>

Additional Options

If you mark the field “Additional Options” on the basic security profile screen with “Y”, a window will be displayed from which you can select the following options:

- **Maintenance Information**
- **Security Notes**
- **Owners**
- **Mailboxes**
- **Activation Dates**
- **Functional Security**
- **Groups/Members**
- **Group Editor**
- **Private Library**
- **Session Options**

The options for which something has already been specified or defined are marked with a plus sign (+).

Some options are only available for certain user types.

You can select one or more items from the window by marking them with any character. For each item selected, an additional window/screen will be displayed (in the order of the items in the selection window).

The Private Library screen can also be invoked directly by pressing PF5 on the basic security profile screen.

The individual options are explained below.

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	<p>In this window, you may enter your notes on the security profile.</p>
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this user security profile.</p> <p>If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For information on owners and co-owners, see the section Countersignatures.</p>
Mailboxes	<p>In this window, you may enter up to five mailbox IDs.</p> <p>For information on mailboxes, see the section Mailboxes.</p>
Activation Dates (A, P, M, G)	<p>In this window, you may define dates as of which or until when the security profile shall be valid.</p> <p>The message “This security profile is currently not active.” is displayed if the security profile is not yet or no longer or temporarily not valid, which means that the corresponding user ID cannot be used before or after a certain date or within a certain period of time.</p>
Functional Security	<p>In this window, you may define functional security for the user with respect to the command processors defined in the libraries the user has access to.</p> <p>This is only relevant if command processors have been created with the Natural utility SYSNCP. See the section Functional Security for details.</p>
Groups/Members (display only)	<p>If you mark this field, a list of all groups to which the user belongs will be displayed.</p> <p>If the user is a GROUP, a list of all users who belong to the GROUP will be displayed.</p>
Group Editor (G)	<p>If you mark this field, the Edit Group Members function will be invoked. This function is explained under Editing Group Members below.</p>
Private Library (A, P)	<p>A user may have a “personal” library whose ID is the same as his/her user ID. Such a library is called a <i>private library</i>.</p> <p>Private libraries can be made available in two modes:</p>

Additional Option	Explanation
	<p>■ Public mode: In this mode, private libraries are treated like any other libraries, that is, their use can be controlled in the same way as that of “normal” libraries. The only difference is that if a private library is protected (which is the default), the user with the same ID can access it without having to be linked to it, while other users need a link to it (see Protecting a Private Library in the section <i>Protecting Libraries</i>).</p> <p>■ Private mode: In this mode, a private library can only be accessed by the user who is directly attached to it, that is, whose user ID is the same as the library ID. Not even a Natural Security administrator has access to it. (The only way for an administrator to gain access to a private library is by modifying the user's password in the user's security profile and then logging on to the private library with the user's user ID and the new password.) Thus, such a private library provides a certain degree of seclusion for the user; and possible misuse of this seclusion is hard to eliminate. Therefore it is recommended that this mode <i>not</i> be used.</p> <p>The mode is set with the general option “Private libraries in public mode” (described in the section <i>Administrator Services</i>) and applies to all private libraries.</p> <p>For information on creating and maintaining a private library, see the section <i>Library Maintenance</i>.</p> <p>As far as access to DDMs/files is concerned, there is no difference between private libraries and “normal” libraries.</p> <p>Note: Unless explicitly stated otherwise, what is said in the Natural Security documentation about libraries also applies to private libraries.</p>
Session Options (A, P, G)	See below.

Session Options

Option	Explanation						
Unlock Objects	<p>This option controls the use of the Natural system command UNLOCK, which is used in conjunction with the Natural Development Server. You can specify one of the following values:</p> <table> <tr> <td>N</td><td>The user cannot use the UNLOCK command.</td></tr> <tr> <td>Y</td><td>The user can use the UNLOCK command, but only for his/her own programming objects (that is, objects locked under his/her user ID).</td></tr> <tr> <td>F</td><td>The user can use the UNLOCK command for any locked programming object.</td></tr> </table> <p>The default value is “Y”.</p>	N	The user cannot use the UNLOCK command.	Y	The user can use the UNLOCK command, but only for his/her own programming objects (that is, objects locked under his/her user ID).	F	The user can use the UNLOCK command for any locked programming object.
N	The user cannot use the UNLOCK command.						
Y	The user can use the UNLOCK command, but only for his/her own programming objects (that is, objects locked under his/her user ID).						
F	The user can use the UNLOCK command for any locked programming object.						

Option	Explanation	
Environment Protection (display only)	This field is only relevant if environment protection is active (that is, if the general option Environment Protection is set to "Y"); it indicates if there are environments which the user is not allowed to access:	
	N	The user can access any environment for which a security profile is defined.
	Y	Access to at least one defined environment is disallowed for the user.
	For details on environment protection, see the section <i>Protecting Environments</i> .	
Suspend Line Protection	This field determines whether or not the user is allowed to use the Natural Studio program editor function "Suspend Line Protection":	
	Y	The user may use the function.
	N	The user cannot use the function.

Creating and Maintaining User Profiles

This section describes the functions used to create and maintain user profiles. It covers the following topics:

- [Invoking User Maintenance](#)
- [Adding a New User](#)
- [Adding Multiple New Users](#)
- [Selecting Existing Users for Processing](#)
- [Copying a User](#)
- [Modifying a User](#)
- [Renaming a User](#)
- [Deleting a User](#)
- [Displaying a User](#)
- [Editing Group Members](#)
- [Copying a User's Links](#)

Invoking User Maintenance

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark the object type "User" with a character or with the cursor. The User Maintenance selection list will be displayed.

From this selection list, you invoke all user maintenance functions as described below.

Adding a New User

The Add User function is used to define new users to Natural Security, that is, create user security profiles.

When you add a new user, you have to specify:

- a user ID,
- a user type,
- the ID of a default profile (optional).

User ID

The user ID is used by Natural Security to identify the user. It may be 1 to 8 characters long. The ID must be unique among all user IDs and library IDs defined to Natural Security. For user IDs, the same naming conventions apply as for [library IDs](#) (see the section *Library Maintenance*).

- If the user is an individual, usually an ID is chosen which is related to the user's name.
- If the user is a terminal, the ID must be identical to the terminal ID by which the terminal is defined to the computer (ask your system programmer).
- If the user is a group, choose whatever ID you like.

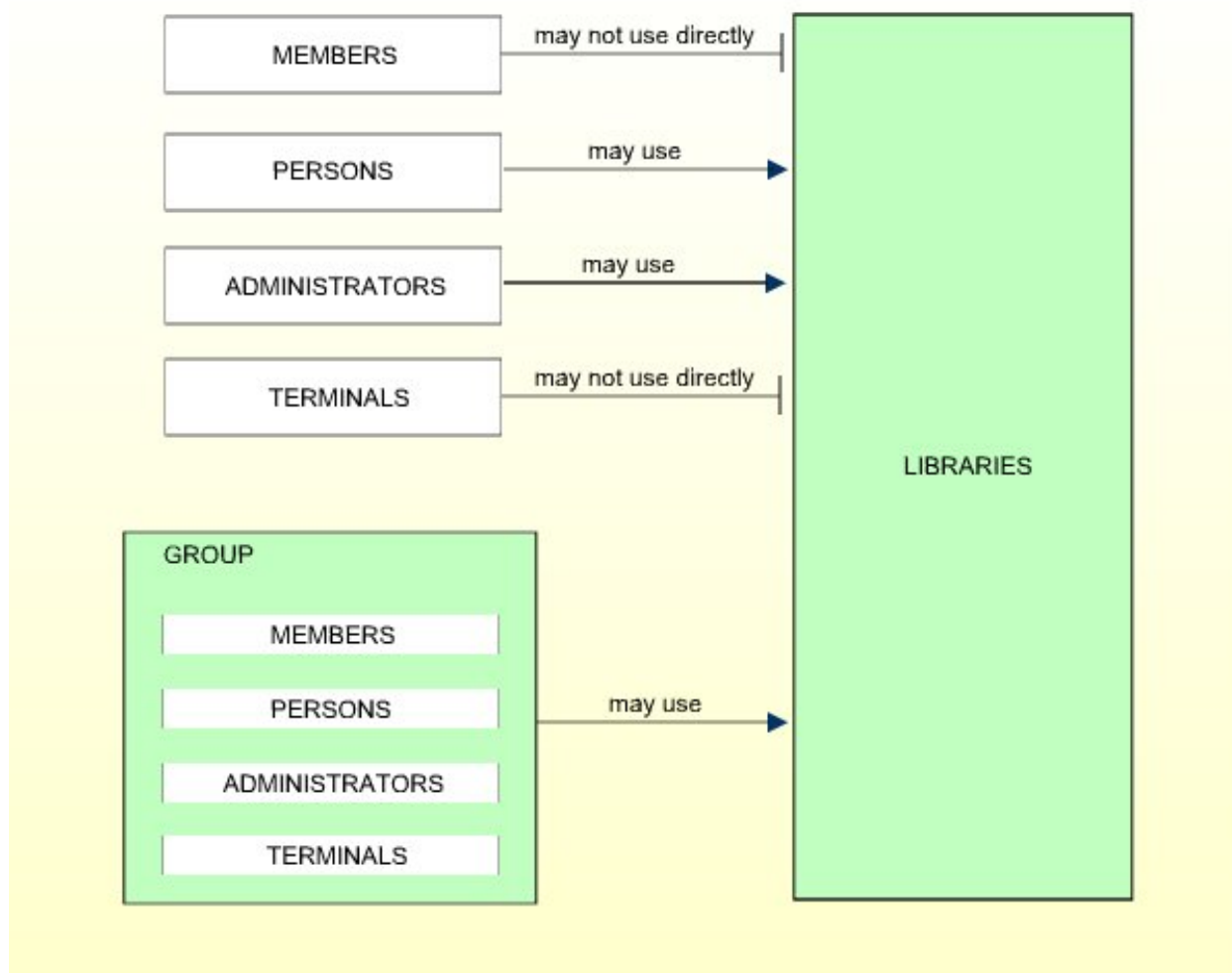
User Type

When you add a user, you specify the code for one of the following user types:

Code	User Type
G	Group
M	Member
P	Person
A	Administrator
T	Terminal
B	Batch User (see Batch User Security Profiles in the section <i>Natural Security In Batch Mode</i>)

If the user to be defined is a group, the user type must be “G”. If the user to be defined is a terminal, the user type must be “T”. If the user to be defined is an individual, the user type should be “M” (except individuals who are Natural Security administrators and have to be user type “A”).

The access rights of different types of users to libraries are summarized in the following diagram:



If you have doubts about the correct user type specification, please refer to [Users](#) in the section *The Structure And Terminology Of Natural Security*.

Once an individual has been defined, you can later change his/her user type classification (as explained under [Upgrading and Downgrading Users](#) below).

Default Profile

When you add a new user, you can either type in every item within the user security profile by hand; or you can use a pre-defined user default profile as a template for the security profile you are creating.

Before you use default profiles, you should be familiar with the "normal" way of defining users (that is, without default profile).

Default profiles are created and maintained in the Administrator Services subsystem.

The *user type* of the default profile you specify must be the same as that of the user security profile you are creating.

If you specify the ID of a default profile in the Add User window, the items from the default profile will be copied into the user profile - except the user ID, user name and the owners.

On the Add User screen, you can then overwrite the items copied into the user profile and specify further items.

For further information, see [User Default Profiles](#) in the section *Administrator Services*.



Note: To define numerous users with identical security profiles, you can also use the Multiple Add User function (see [Adding Multiple New Users](#) below).

How to Add a New User

In the command line of the User Maintenance selection list, you enter the command:

ADD

A window will be displayed. In this window, you enter the following:

- a user ID,
- a user type,
- the ID of a default profile (optional).

The Add User screen for the specified user type will be displayed. On this screen, you define a security profile for the user.

The Add User screen and the subsequent screens/windows that are part of a user security profile as well as the individual items you may define are described under [Components of a User Profile](#) above.

When you add a new user, the owners specified in your own user security profile will automatically be copied into the user security profile you are creating.

Adding Multiple New Users

Before you use the Multiple Add User function you should be familiar with the "normal" way of defining users (as described under [Adding a New User](#) above).

The Multiple Add User function allows you to define large numbers of users to Natural Security in a fast and easy way. You can use this function to define numerous users who are to have identical security profiles.

In the command line of the User Maintenance selection list, you enter the command:

ADDM

A window will be displayed. In this window, enter a *user ID* and a *user type* specification (and, optionally, the ID of a *default profile*).

The Multiple Add User screen for the specified user type will be displayed. On this screen you may define a security profile for the user.

The Multiple Add User screen and the subsequent screens/windows that are part of a user security profile as well as the individual items you may define are described under [Components of a User Profile](#) above.

When you add a new user, the owners specified in your own user security profile will automatically be copied into the user security profile you are creating.

► To create multiple user security profiles

- 1 On the first screen (and any additional screens/windows), you define a security profile for one user.
- 2 Once you have finished typing in the items to be defined and are back on the Multiple Add User screen without any additional screens/windows being active, press ENTER. The first user is now defined.
- 3 Then press PF5 - the same security profile will be displayed again omitting the user ID and user name entries. Type in a user ID and the name of the next user and press ENTER. The second user is now defined.
- 4 Then press PF5 - the same security profile will be displayed again omitting the user ID and user name entries. In this manner, you may continue to define more users all with identical security profiles.
- 5 To leave the Multiple Add User function, press PF3.

Selecting Existing Users for Processing

When you invoke User Maintenance, a list of all users that have been defined to Natural Security will be displayed.

If you do not wish to get a list of all existing users but would like only certain users to be listed, you may use the Start Value and Type/Status options as described in the section [Finding Your Way In Natural Security](#).

On the Main Menu, enter code “M” for “Maintenance”. A window will be displayed. In the window, mark the object type “User” with a character or with the cursor (and, if desired, enter a start value and/or user type). The User Maintenance selection list will be displayed:

11:11:11

*** NATURAL SECURITY ***

2009-07-31

- User Maintenance -

Co	User ID	User Name	Type	Message
—	AAZ	ABDUL ALHAZRED	A	
—	AD	ARTHUR DENT	A	
—	CDW	CHARLES DEXTER WARD	A	
—	CZ	CODY ZAMORA	P	
—	DI	DAVID INNES	A	
—	EW	ESMERALDA WEATHERWAX	M	
—	HC	HAGBARD CELINE	A	
—	HW	HENRY WILT	A	
—	IW	IRENE WILDE	M	
—	LL	LOCKE LAMORA	M	
—	PE	PALMER ELDRITCH	M	
—	PR	PRECIOUS RAMOTSWE	M	
—	SV	SAM VIMES	M	
—	TN	THURSDAY NEXT	P	
—	VV	VINCENT VEGA	M	

Command ==>

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12---

HelpExitFlip - +Canc

For each user, the user ID, user name and user type are displayed.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

The following user maintenance functions are available (possible code abbreviations are underlined):

Code	Function
<u>C</u> O	Copy user
<u>M</u> O	Modify user
R <u>E</u>	Rename user
D <u>E</u>	Delete user
<u>D</u> I	Display user
E <u>G</u>	Edit group members
L <u>A</u>	Link user to applications
L <u>L</u>	Link user to libraries
L <u>O</u>	Link user to external objects
C <u>P</u>	Copy user's links
E <u>P</u>	Protect environments for user
M <u>D</u>	Modify DDM restrictions in user's private library (this function is not available on mainframes)

To invoke a specific function for a user, mark the user with the appropriate function code in column "Co".

You can select various users for various functions at the same time; that is, you can mark several users on the screen with a function code. For each user marked, the appropriate processing screen will be displayed. You can then perform for one user after another the selected functions.

Copying a User

The Copy User function is used to define a new user to Natural Security by creating a security profile which is identical to an already existing user security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - *except*:

- the user name (see *How to Copy* below),
- the password,
- the ETID (which identifies End of Transaction data),
- the owners (these will be copied from your own user security profile into the new user security profile you are creating).

Whether the groups entered in the "Privileged Groups" column and any links to libraries are copied depends on whether you copy with or without links (see below).

How to Copy

On the User Maintenance selection list, mark the user whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, specify the following:

To user	Enter the ID of the "new" user.
User name	This field shows the name of the existing user. Overwrite it with the name of the "new" user.
With links	If you wish links <i>not</i> to be copied, leave the "N" in this field untouched; if you wish any links existing for the existing user also to apply to the new user, type in a "Y". See below for details.

The Copy User screen will be displayed showing the new security profile.

The Copy User screen and the subsequent screens/windows that are part of a user security profile as well as the individual items you may define are described under [Components of a User Profile](#) above.

Copying Without Links

If you leave the "N" in the "with links" field of the Copy User window:

- the groups entered in the Privileged Groups column of the existing user will not be copied into the new user security profile;
- any links defined for the existing user will not apply to the new user;
- any user-specific and user-library-specific utility profiles for the existing user will not apply to the new user.

Copying With Links

If you enter a "Y" in the "with links" field of the Copy User window:

- any links that existed for the existing user are copied for the new user, and you have the option to cancel the links you wish not to apply for the new user;
- the new user will be added to all groups in which the existing user is contained (and all access right of the groups to libraries then also apply for the new user), and you have the option to delete the new user from any of these groups;
- any user-specific and user-library specific utility profiles that existed for the existing user are copied for the new user.

The procedure is as follows:

1. Once you have made any changes to the copied security profile and then leave the Copy User screen by pressing PF3, a list of libraries is displayed: the list contains all libraries to which the existing user is linked directly.
2. On the list, you may mark individual libraries with "CL" to cancel any links you wish *not* to apply for the new user; to all libraries you do not mark, the new user will automatically be linked in the same manner - normal or special link - as the existing user.
3. Once you have established all direct links and then leave the list of libraries by pressing PF3, a list of groups is displayed: the list contains all groups in which the existing user is contained.
4. On the list you may mark with "CL" the groups to which you wish the new user *not* to be added; the new user will automatically be added to all groups you do not mark. If any of the groups to which the new user is added is entered as "Privileged Group" in the security profile of the existing user, they will automatically also be entered as "Privileged Groups" in the new user security profile.

Modifying a User

The Modify User function is used to change an existing user security profile.

On the User Maintenance selection list, mark the user whose security profile you wish to change with function code "MO". The Modify User screen will be displayed.

The Modify User screen and the subsequent screens/windows that are part of a user security profile as well as the individual items you may define or modify are described under [Components of a User Profile](#) above.

Upgrading and Downgrading Users

If need be, you may change the user type classification of an individual.

If you wish to change the user type, first type in the new user type and press ENTER to obtain the appropriate Modify User screen before you further modify the security profile, because the Modify User screens for the different user types are not identical to one another.

Upgrading a User

You may "promote" a MEMBER to become a PERSON or an ADMINISTRATOR; and you may "promote" a PERSON to become an ADMINISTRATOR.

Downgrading a User

You may downgrade an ADMINISTRATOR to become a PERSON or a MEMBER; and you may downgrade a PERSON to become a MEMBER.

- Before you can downgrade a user from ADMINISTRATOR to PERSON, you have to remove him/her as owner from every security profile in which he/she is specified as owner. As long as an ADMINISTRATOR is still owner of any security profile, he/she cannot be downgraded.

- Before you can downgrade a user from ADMINISTRATOR to MEMBER, you have to perform the following:
 - You have to remove him/her as owner from every security profile in which he/she is specified as owner. As long as an ADMINISTRATOR is still owner of any security profile, he/she cannot be downgraded.
 - You have to cancel all direct links from the user to libraries/external objects. As long as the user is linked to any library or external object, he/she cannot become a MEMBER.
 - You have to delete the ADMINISTRATOR's private library (if defined). As long as the user has a private library, he/she cannot become a MEMBER.
- Before you can downgrade a user from PERSON to MEMBER, you have to cancel all direct links from the user to libraries/external objects. As long as the user is linked to any library or external object, he/she cannot become a MEMBER. In addition, you have to delete the PERSON's private library (if defined). As long as the user has a private library, he/she cannot become a MEMBER.

User Locked?

When the **“Lock User Option”** (described in the section *Administrator Services*) is active, it may occur that the user security profile has been locked.

If the security profile is locked, this will be indicated on the Modify User screen by the message:

This user is currently locked due to logon/countersign error!

If you enter a “Y” in the “Unlock? (Y/N)” field, a window will be displayed which provides detailed information on how and when the locking occurred. In that window you may also unlock the security profile.



Note: You may also view and unlock locked users by means of the **“List/Unlock Locked Users”** function (which is described in the section *Administrator Services*).

Renaming a User

The Rename User function allows you to change the user ID of an existing user security profile.

On the User Maintenance selection list, you mark the user whose ID you wish to change with function code “RE”. A window will be displayed in which you can enter a new ID for the user (and, optionally, change the user's name).

An ADMINISTRATOR who is an owner of one or more security profiles cannot be renamed. A user who is specified as DDM modifier in one or more DDM/file security profiles, cannot be renamed either.

Deleting a User

The Delete User function is used to delete an existing user security profile.

On the User Maintenance selection list, you mark the user you wish to delete with function code “DE”. A window will be displayed.

- If you have invoked the Delete User function and should then decide against deleting the given user security profile, leave the Delete User window by pressing ENTER without having typed in anything.
- If you wish to delete the given user security profile, enter the user's ID in the window to confirm the deletion.

Depending on the setting of the general option **“Allow Deletion of Users Who Are Owners/DDM Modifiers”** (described in the section *Administrator Services*), it may not be possible to delete a user security profile if the user is specified as owner in any security profile or as DDM modifier in any DDM/file security profile.

If you mark more than one user with “DE”, a window will appear in which you are asked whether you wish to confirm the deletion of each user security profile by entering the user's ID, or whether all users selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a user accidentally.



Note: If you delete a GROUP security profile, this will *not* delete the individual security profiles of the users assigned to this GROUP.

Displaying a User

The Display User function is used to display an existing user security profile.

On the User Maintenance selection list, mark the user whose security profile you wish to view with function code “DI”. The Display User screen will be displayed.

The items displayed on the Display User screen and any additional windows that are part of a user security profile are explained under **Components of a User Profile** above.

User Locked?

When the **“Lock User Option”** (described in the section *Administrator Services*) is active, it may occur that the user security profile has been locked.

If the security profile is locked, this will be indicated on the Display User screen by the message:

This user is currently locked due to logon/countersign error!

If you enter a “Y” in the “Lock Info (Y/N)” field, a window will be displayed which provides detailed information on how and when the locking occurred.

Editing Group Members

The Edit Group Members function is used to assign users to or delete users from a group.

As long as the number of users assigned to a group does not exceed 5, the group members may be maintained in the “Members” column of the group's security profile by using the Modify User function. For larger groups, membership maintenance has to be done with the Edit Group Members function.

You can invoke the Edit Group Members function either from the User Maintenance selection list or from within a group's security profile:

- On the User Maintenance selection list, mark the group you wish to edit with function code “EG”.
- In a group's security profile, mark the option “Group Editor” in the Additional Options window with any character.

The Edit Group Members screen will be displayed:

>	> + Gr ELGRUPO		Size 5	Line 1
ALL	User ID	User Name	Type	Status
	-----	-----	-----	-----
	AD	ARTHUR DENT	A	
	AT	TIFFANY ACHING	A	
	MT	MERCY THOMPSON	M	
	RM	RACHEL MORGAN	M	
	T2112	WEINRIB'S TERMINAL	T	

The Edit Group Members screen is a modified Natural program editor. When you invoke it, the users already contained in the given group are read into the source area. The list of group members will be in alphabetical order of user IDs. For each user, the user ID, user name and user type are displayed.

To add a user to the group, add the user ID to the list. To delete a user from the group, delete the user ID from the list.

Remember that users have to be defined to Natural Security before they can be added to a group.

It does not matter in which order you add new user IDs: when you catalog the list of group members (see command CAT below), they will automatically be sorted alphabetically.

To edit the list, you can use the Natural program editor scrolling commands, line commands and editor commands (as described in the Natural *Editors* documentation).

To add *all* users contained in one group to the group you are editing, enter the command `INCLUDE group-ID` in the command line of the Edit Group Members screen. All users contained in the group whose ID you specify with the `INCLUDE` command will then be added to the list. They will be included before the user who is displayed in the top line of the screen.

Remember that a user of type "group" must not be contained within another group.

Modifications are only processed in the source area until you enter the command `CAT[ALOG]` in the command line (or press PF3). This command first invokes a procedure which checks for duplicate IDs. If the IDs are unique, the edited list of members will be entered in the group's security profile.

With the command `CHECK` you invoke the checking procedure only.

When you perform the `CATALOG` function, the user exit `NSCUSEX2` is invoked. It displays a list of the group's members, indicating which members have been added to the group and which have been removed from it.

To leave the Edit Group Members screen, enter a period (.) in the command line.

Copying a User's Links

The Copy User's Links function is used to copy links from one existing user profile to another one of the same user type.

You can individually select the links to be copied. In addition to links, you can copy group memberships (including "Privileged Groups" specifications) and functional security definitions.

On the User Maintenance selection list, you mark the user whose links you wish to copy with function code "CP". A window will be displayed in which you enter the ID of the user to which you wish to copy links. In addition, you can restrict the selection of link types in the window:

- Library links
- Groups/Members
- Utility links
- Functional security
- File links (if the user has a private library)
- Environment links
- External object links

By default, all the above are selected. To deselect one type, you remove the "X".

A list of all the first user's existing links (of the selected types) will then be displayed.

The listed links are not automatically preselected for copying. In the “Co” column of the list, you have to mark with function code “CO” each link you wish to be copied from the one user to the other.

You can mark one or more links per screen. For each link marked, a message indicating if it has been copied will be displayed. If a link cannot be copied, this will also be indicated. For example, if the user already has a link to a specific object, this cannot be replaced by a link copied from the other user.

8 Library Maintenance

■ Components of a Library Profile	120
■ Creating and Maintaining Library Profiles	145

A library is defined to Natural Security by creating a *library security profile*. The library security profile determines the conditions under which the library may be used.

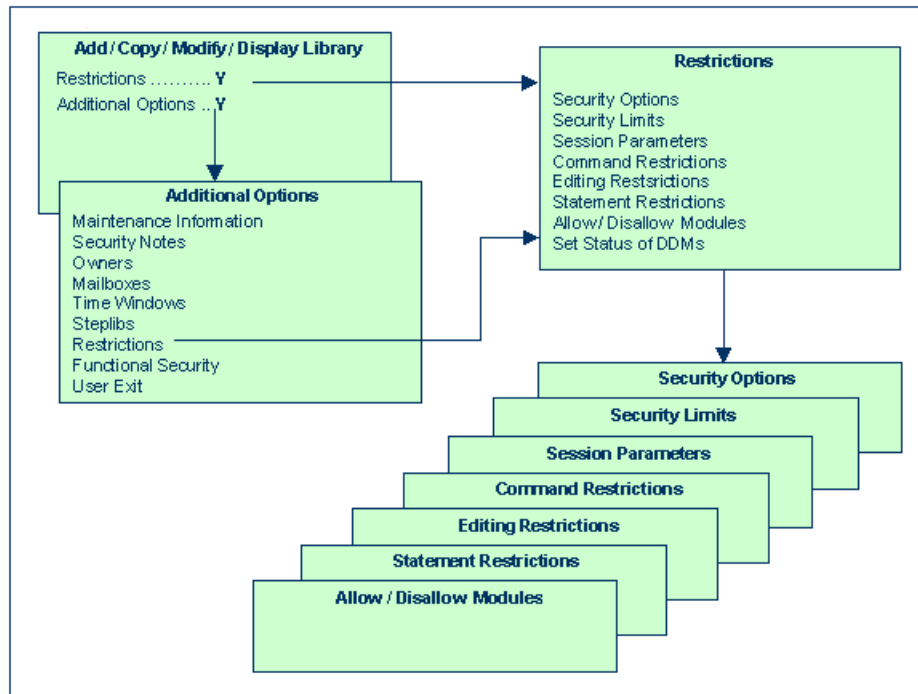
This section covers the following topics:

Components of a Library Profile

This section covers the following topics:

- Overview of Components
- Components on Main Library-Profile Screen
- General Options
- Library File
- Transactions
- Additional Options
- Restrictions
 - Security Options
 - Security Limits
 - Session Parameters (including RPC Restrictions)
 - Command Restrictions
 - Editing Restrictions
 - Statement Restrictions
 - Allow/Disallow modules
 - Set Status of DDMs

Overview of Components



Components on Main Library-Profile Screen

The following type of screen is the "basic" library security profile screen, which appears when you invoke one of the functions Add, Copy, Modify, Display for a library security profile:

```

14:00:00                *** NATURAL SECURITY ***                2009-07-31
                        - Modify Library -

                                Modified .. 2009-07-20 by SAG

Library ID ..... TESTLIB
Library Name ... _____

      General Options      Library File      Transactions
      -----
People-protected .... Y   DBID ..... _____   Startup ..... _____
Terminal-protected .. N   FNR ..... _____   Batch execution .. Y
Restrictions ..... Y     Password .... _____   Restart ..... _____
Logon recorded ..... Y   Ciphercode .. _____   Error ..... _____
Utilities ..... 0                                     User exit ..... _____
Programming mode .... R
Cross-reference ..... N
Restart ..... Y
  
```

Additional Options ... N

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

The individual items you may define as parts of a library security profile are explained below.

Field	Explanation
Library ID (display only)	The ID of the library as specified when the library security profile was created.
Library Name	You may enter a name for the library, which may be up to 32 characters long.

General Options

Field	Explanation				
People-protected/ Terminal-protected	You may specify whether the library is to be <i>people-protected</i> and/or <i>terminal-protected</i> in order to restrict the use of the library. The possible combinations of protection are described under Protected Libraries in the section <i>Protecting Libraries</i> .				
Restrictions	<p>Special restrictions may be defined for the library, as described under Additional Options below.</p> <ul style="list-style-type: none"> ■ If no restrictions are defined, the system profile defined in the Natural parameter module applies. ■ If restrictions are defined, the value of this field is automatically set to "Y". If you set it to "N" again, any specification you have made in the restrictions will automatically be deleted! 				
Logon recorded	<p>This option determines whether logons to the library are to be recorded or not.</p> <table> <tr> <td>Y</td><td>Every time a user logs on to the library, a logon record will be written by Natural Security. You may review the activities of users by viewing these logon records (see Logon Records in the section <i>Administrator Services</i> for further information).</td></tr> <tr> <td>N</td><td>Logons to the library will not be recorded.</td></tr> </table>	Y	Every time a user logs on to the library, a logon record will be written by Natural Security. You may review the activities of users by viewing these logon records (see Logon Records in the section <i>Administrator Services</i> for further information).	N	Logons to the library will not be recorded.
Y	Every time a user logs on to the library, a logon record will be written by Natural Security. You may review the activities of users by viewing these logon records (see Logon Records in the section <i>Administrator Services</i> for further information).				
N	Logons to the library will not be recorded.				
Utilities	<p>For consistent control of Natural utility usage, <i>utility profiles</i> should be used; they are described in the section Protecting Utilities.</p> <p>This option applies to the following Natural utilities:</p> <ul style="list-style-type: none"> ■ SYSERR (as well as NATLOAD, NATUNLD and SYSTRANS) - if no utility profile is defined for this utility; ■ SYSMAIN - if no utility profile is defined for SYSMAIN; or if the Session Option "Utilities Option" is set to "Y" or "O" in the default security profile of the SYSMAIN utility. 				

Field	Explanation	
	<p>■ SYSOBJH - if the Session Option "Utilities Option" is set to "Y" or "O" in the default security profile of the SYSOBJH utility.</p> <p>Under this condition, this option determines who may use the utility to process the contents of the library.</p> <p>Possible values are:</p>	
	N	No protection - The library's contents may be processed by any user.
	O	<p>Permission for Owners - The library's contents may be processed only by the <i>owners</i> of the library security profile. If no owner is specified, any user of type ADMINISTRATOR may do so. In the case of a private library, in addition to the owners, the user with the same ID as the library ID may also process the library's contents.</p> <p>In batch mode, an owner who requires a countersignature from a co-owner cannot process the contents of the library (as countersignatures are not possible in batch mode).</p> <p>In online mode, if the Session Option "Utilities Option" is set to "O" in the default security profile of SYSMAIN or SYSOBJH, and an owner requires a countersignature, the countersignature prompt will be suppressed and the library excluded from SYSMAIN/SYSOBJH processing.</p>
	P	<p>Permission under Protection rules - The library's contents may be processed under <i>protection rules</i>, that is, only by users who are allowed to log on to the library. For private libraries in private mode, the following applies: The user with the same ID as the library ID may process the library's contents; anyone else may process it only after entering that user's password (on a countersignature screen provided for that purpose). In batch mode, please note that a user cannot process the contents of another user's private library in private mode (as no password can be entered in batch mode).</p>
	<p>If the Natural system command SCAN is allowed for the library (see Command Restrictions below), this option also applies to the SCAN command.</p>	
Programming mode	Natural programming mode:	
	S	(= Structured mode) - The programming mode to be used cannot be changed with the Natural parameter SM, and structured mode will invariably be in effect.

Field	Explanation	
	R	(= Reporting mode) - The setting of the Natural profile/session parameter SM (described in the <i>Natural Parameter Reference</i> documentation) determines the mode to be used.
Cross-reference	This option determines whether an active cross-reference in Predict (if installed) will be generated for the library.	
	Y	Yes - An active cross-reference will be generated.
	N	No - An active cross-reference will not be generated.
	F	Force - An active cross-reference will be forced.
	D	Doc - Objects to be cataloged must be documented in Predict. However, no active cross-reference will be generated.
	See the Predict documentation for details on active cross-references.	
Restart	Y	The library may be re-invoked by entering "RESTART" as the library ID on the logon screen; an Adabas OPEN command with End of Transaction ID (ETID) will be executed during the logon procedure.
	N	The library cannot be "RESTARTed". The ETID specified in Natural Security will not be used for the Adabas OPEN command.
Version control (display only)	<p>This field only applies on mainframe computers and if the library is under control of Predict Application Control.</p> <p>This field indicates the version control status of the library. If the library is controlled by Predict Application Control, the database ID (DBID) and file number (FNR) of the FDIC system file in which the library's Predict data are stored are also displayed.</p>	

Library File

The items under Library File concern the database file where the source programs and object modules contained in the library are to be stored.

Field	Explanation
DBID/FNR	<p>The database ID and file number of the file.</p> <p>If no DBID/FNR are specified here, the DBID/FNR of the FUSER parameter as defined in the Natural parameter module/file apply (see the FUSER parameter in the <i>Natural Parameter Reference</i> documentation).</p>
Password	<p>This field only applies on mainframe computers, it has no effect under UNIX, OpenVMS and Windows.</p> <p>If the library file is password-protected, the Adabas password (for VSAM files, the VSAM DDname) must be entered in this field to enable Natural to access the file.</p>

Field	Explanation
Cipher code	This field only applies on mainframe computers, it has no effect under UNIX, OpenVMS and Windows. If the library file is ciphered, the Adabas cipher code (for VSAM files, the VSAM password) must be entered in this field to enable Natural to access the file.
Read-only	If you wish the library file to be read-only, mark this field with an "X" (this corresponds to the RO option of the FUSER profile parameter).
ETID (display only)	This field contains the library-specific component of the ID for End of Transaction data (for details on ETIDs, see Components of a User Profile in the section <i>User Maintenance</i>).



Note: For the Natural system libraries - that is, all libraries whose IDs begin with "SYS" (except the library SYSTEM) - you cannot enter a DBID, FNR, password, or cipher code. For these libraries the DBID, FNR, password, and cipher code of the Natural profile parameter FNAT (described in the *Natural Parameter Reference* documentation) as defined in the Natural parameter module/file invariably apply.

Transactions

Field	Explanation						
Startup	You can enter the name of a startup transaction; this transaction will always be invoked immediately after a successful logon to the library. See also the Natural system variable *STARTUP. The name of the startup transaction will be placed in the Natural system variable *STARTUP. If it is also executed in batch mode, its name will only be placed into *STARTUP if "Batch execution" (see below) is set to "S".						
Batch execution	This field only applies if the Natural system variable *DEVICE is set to "BATCH" (otherwise its value has no effect). It determines whether the startup transaction specified in the library profile (see above) is also executed in batch mode. You can specify one of the following values: <table border="1"> <tr> <td>Y</td><td>The startup transaction will also be executed (once) in batch mode.</td></tr> <tr> <td>S</td><td>The startup transaction will also be executed in batch mode; in addition, its name will be placed in the Natural system variable *STARTUP.</td></tr> <tr> <td>N</td><td>If the NEXT/MORE line is allowed for the library (see Security Options below), the startup transaction will <i>not</i> be executed in batch mode. If the NEXT/MORE line is <i>not</i> allowed, the startup transaction will also be executed (once) in batch mode.</td></tr> </table> See also the section Natural Security In Batch Mode .	Y	The startup transaction will also be executed (once) in batch mode.	S	The startup transaction will also be executed in batch mode; in addition, its name will be placed in the Natural system variable *STARTUP.	N	If the NEXT/MORE line is allowed for the library (see Security Options below), the startup transaction will <i>not</i> be executed in batch mode. If the NEXT/MORE line is <i>not</i> allowed, the startup transaction will also be executed (once) in batch mode.
Y	The startup transaction will also be executed (once) in batch mode.						
S	The startup transaction will also be executed in batch mode; in addition, its name will be placed in the Natural system variable *STARTUP.						
N	If the NEXT/MORE line is allowed for the library (see Security Options below), the startup transaction will <i>not</i> be executed in batch mode. If the NEXT/MORE line is <i>not</i> allowed, the startup transaction will also be executed (once) in batch mode.						

Field	Explanation
Restart	You can enter the name of a restart transaction; this transaction will always be invoked when the library is reinvoked by entering "RESTART" as the library ID on the logon screen.
Error	<p>You can enter the name of an error transaction. This transaction will be invoked after the occurrence of an execution time error (if the program does not contain an ON ERROR statement, or if it does contain an ON ERROR block which is not exited with a FETCH, STOP, TERMINATE or RETRY statement); if the Natural profile parameter SYNERR=ON is set, the error transaction may also handle syntax errors.</p> <p>For further information on error transactions, see <i>Using an Error Transaction Program</i> in the <i>Natural Programming Guide</i>.</p> <p>Note: If no error transaction is specified here, the program specified with the Natural profile parameter ETA (described in the <i>Natural Parameter Reference</i> documentation) will receive control when an error occurs. If an error occurs during an initial logon, the program specified with the ETA parameter will also receive control (for other logon errors, the error transaction specified in the library <i>from which</i> you log on to another library applies).</p>

User Exit

With each library profile and special link profile, you can store 250 bytes of additional data of your choice.

These additional data can be stored/read by means of a user exit subprogram which must contain a CALLNAT statement (with five parameters as described below) which in turn invokes one of the following subprograms:

- SNAASEXT - to store additional library data,
- SNAAREXT - to read additional library data,
- SNAUSEXT - to store additional special link data,
- SNAUREXT - to read additional special link data.

These four subprograms are contained in the Natural Security library SYSSEC.

In the User Exit field of the library profile or special link profile, you enter the name of the user exit that invokes one of the above subprograms.

To invoke the user exit, you mark "User Exit" with "Y" in the **Additional Options** window (see below).

If you wish to handle the additional data from within a library, you can also invoke the above subprograms by means of a user exit from a library itself. In this case you must copy the subprograms into that library (by using the SYSMAN utility). When invoked from a library, each subprogram will check and ensure that only data concerning that library or the specified link are read/stored.

In the security profiles of the Natural system libraries, that is, all libraries whose IDs begin with “SYS” (except the library SYSTEM), you cannot specify a user exit.

SNAASEXT

SNAASEXT is used to store additional library data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAASEXT	Contents returned from SNAASEXT
1st	A8	none	Library ID
2nd	A32	none	Library name
3rd	D	none	Date of latest modification
4th	A250	Data to be stored	same as passed
5th	B2	none	Return code

SNAAREXT

SNAAREXT is used to read additional library data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAAREXT	Contents returned from SNAAREXT
1st	A8	none	Library ID
2nd	A32	none	Library name
3rd	D	none	Date of latest modification
4th	A250	none	Data read
5th	B2	none	Return code

When you invoke SNAAREXT or SNAASEXT from a library profile in SYSSEC, the data will refer to the library you are currently maintaining.

When you invoke SNAAREXT or SNAASEXT from outside SYSSEC, the data will refer to the library from which you invoke the subprogram.

SNAUSEXT

SNAUSEXT is used to store additional special link data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAUSEXT	Contents returned from SNAUSEXT
1st	A8	none	Library ID
2nd	A8	User ID (must only be filled if SNAUSEXT is invoked from outside SYSSEC)	User ID
3rd	D	none	Date of latest modification
4th	A250	Data to be stored	same as passed
5th	B2	none	Return code

SNAUREXT

SNAUREXT is used to read additional special link data. It must be invoked with the following five parameters:

Parameter	Format/Length	Contents passed to SNAUREXT	Contents returned from SNAUREXT
1st	A8	none	Library ID
2nd	A8	User ID (must only be filled if SNAUREXT is invoked from outside SYSSEC)	User ID
3rd	D	none	Date of latest modification
4th	A250	none	Data read
5th	A2/B2	*	Return code *

* When you invoke SNAUREXT from outside SYSSEC, you may read several special links to the library by using the 2nd parameter as start value and specifying one of the following operators in the 5th parameter (A2): "EQ", "=", "GT", ">", "LT", "<", "GE", ">=", "LE", "<=". These operators determine the read condition as compared against the 2nd parameter. Return code (B2) "0" indicates that the specified special link has been found; any other value indicates that no such link has been found.

When you invoke SNAUREXT or SNAUSEXT from a special link profile in SYSSEC, the data will refer to the link you are currently maintaining. When you invoke SNAUREXT or SNAUSEXT from outside SYSSEC, the data will refer to the link between the specified user ID and the library from which you invoke the subprogram.

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- **Maintenance Information**
- **Security Notes**
- **Owners**
- **Mailboxes**
- **Time Windows**
- **Steplibs**
- **Restrictions**
- **Functional Security**
- **User Exit**

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window/screen will be displayed (in the order of the items in the selection window).

The Restrictions window can also be invoked directly by pressing PF5 on the basic security profile screen.

The individual options are explained below.

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.

Additional Option	Explanation
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this security profile. If no owner is specified, any user of type ADMINISTRATOR may maintain the library.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures.</p>
Mailboxes	<p>In this window, you may enter up to five mailbox IDs. For information on mailboxes, see the section Mailboxes.</p>
Time Windows	<p>In this window, up to five time windows may be specified, outside of which the library cannot be used.</p> <p>When the end of a time window is reached, the application contained in the library will automatically be terminated and Natural Security will perform a logoff. Depending on the general option “Enable Error Transaction Before NAT1700/1701 Logoff”, the application's ON ERROR handling and/or error transaction may be processed before the logoff.</p> <p>For example, if a time window is set to “0815 - 1300”, a user may log on to the library only between 08:15 h and 13:00 h; if a user is still logged on to the library at 13:00 h, the application contained in the library will be terminated.</p>
Steplibs	<p>In this window, you can enter the IDs of the libraries which are to be the steplib libraries (concatenated libraries) for the library. The libraries whose IDs you specify must be defined in Natural Security.</p> <p>Multiple steplibs allow you to make different modules available to different libraries and also restrict the general availability of modules without having to have multiple copies of the same module in multiple libraries; that is, each module has to exist only once, but you can nonetheless make it available to several libraries, but not to others.</p> <p>For example, the modules that are to be available to all libraries can be contained in a general steplib which is specified in all library profiles, while modules that are to be available only to some libraries can be contained in another steplib which is specified only in some library profiles.</p> <p>Moreover, by specifying different special links to a library (see Linking Users to Libraries in the section <i>Protecting Libraries</i>), you can allow different users of the same library the use of different steplibs.</p> <p>You can specify up to 8 steplibs, plus a value for the Natural system variable *STEPLIB: When a programming object is requested in the library but not found in it, the 8 steplibs are searched - in the order in which they are specified in the library profile - for that object. If the requested object cannot be found in any of the 8 steplibs, the *STEPLIB library will be searched for it. If it cannot be found in that library either, the library SYSTEM will be searched for it (without SYSTEM having to be specified as a steplib in a library profile). If no value is specified in any of the 8 steplib fields in the library profile, the 8 steplibs specified with the Natural profile parameter STEPLIB will be used instead.</p>

Additional Option	Explanation
	<p>If no value is assigned to *STEPLIB in the library profile, the *STEPLIB value of the Natural profile parameter STEPLIB will be used instead.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. Owner logic applies to the specification of a steplib; that is, if owners are specified in a library profile (see above), only these owners will be allowed to enter the library as steplib in the profile of another library. 2. For Natural system libraries (that is, libraries whose IDs begin with "SYS") - except library SYSTEM - you cannot specify a *STEPLIB library. For these libraries, an internal system steplib is used as *STEPLIB library. 3. If you use the library SYSTEM as steplib only, SYSTEM itself need not be defined as a library to Natural Security. <p>Dynamic Change of Steplib Table at Runtime</p> <p>The table of steplibs as outlined above is fixed and cannot be changed by the application itself; this means that the same steplib table applies to all users who use the library.</p> <p>Via the Natural application programming interface (API) USR4025 (contained in the library SYSEXT), however, it is possible to dynamically change individual entries in the steplib table. To make use of this possibility, you have to adjust the steplib table as follows: Instead of an actual steplib ID, you specify "*****" (8 asterisks) in a field of the steplib window. At runtime, the actual steplib ID for this position is then supplied by the application via the API.</p> <p>You can specify "*****" in one or more fields of the steplib table. The API only overwrites those fields in the steplib table which contain "*****"; any fields containing actual steplib IDs (or blanks) are not affected by the API.</p> <p>Dynamic steplib assignment is only possible for the steplibs which are last in the sequence of steplibs. This means that in the steplib table, after any field(s) containing "*****", there must be no field containing an actual steplib ID.</p> <p>Thus it is possible, for example, to have a setup where the 1st to 4th steplibs are fixed as specified in the library profile, and the 5th and 6th steplibs are supplied dynamically by the API.</p> <p>DBID, FNR, Password and Cipher Code</p> <p>Next to each steplib name, you can enter a database ID (DBID), file number (FNR), password and cipher code in the steplib window of a library window. If you assign "99999" as DBID value for a steplib in the steplib window of a library profile, the DBID value specified in the library profile of the steplib will be used. The same applies to FNR, password and cipher code values. If you assign no DBID value (or "0") for a steplib in the steplib window of a library profile, the DBID value of that library will be used. The same applies to FNR, password and cipher code values.</p>

Additional Option	Explanation
	By marking a steplib name with the cursor and pressing PF5 in the steplib window of a library profile, you can copy the actual values of DBID, FNR, password and cipher code from the steplib profile into the steplib window. For the *STEPLIB library specified in a library profile, the DBID, FNR, password and cipher code values of that library profile apply.
Restrictions	<p>As part of the restrictions, you may define:</p> <ul style="list-style-type: none"> ■ Security Options ■ Security Limits ■ Session Parameters (including RPC Restrictions) ■ Command Restrictions ■ Editing Restrictions ■ Statement Restrictions ■ Allow/Disallow modules ■ Set Status of DDMs <p>These items are described below.</p>
Functional Security	In this window, you may define functional security for the command processors of the library. This is only relevant if command processors have been created with the Natural utility SYNCP. See the section <i>Functional Security</i> for details.
User Exit	If a user exit is specified in the Transactions column of the main library security profile screen, you can activate that user exit by marking this field.

Security Options

If you mark “Security Options” in the Restrictions selection window with any character, the Security Options window will be displayed. In this window, you can set the following options:

Option	Explanation	
Allow NEXT/MORE line	Y	Allows the use of the Natural main menu.
	N	Suppresses the Natural main menu; when a user logs on to the library, the startup transaction specified for the library will be invoked instead (if no startup transaction is specified, the logon procedure will be invoked; see also the Natural system variable *STARTUP).
Allow system commands	Y	Allows the use of Natural system commands in the library. To disallow individual commands, you use the Command Restrictions section of the library profile (see below).
	N	Disallows the use of all system commands in the library. (This does not affect the system commands FIN, LAST, LASTMSG, LOGOFF, LOGON, MAINMENU, RENUMBER, RETURN, SETUP and TECH; they can always be used.)

Option	Explanation	
Execution of update programs	Y	Programs that update the database can be executed in the library.
	N	Programs that update the database cannot be executed in the library.
Device	<p>If this field is left blank, use of the library will not be restricted to any operation mode or device.</p> <p>If you enter a value, use of the library will be restricted to one specific device or operation mode. Possible values are: ASYNCH, BATCH, BTX, COLOR, PC, TTY, VIDEO and WS-CON (according to the current values of the Natural system variable *DEVICE).</p>	
Clear source area by logon	N	The editor source work area will <i>not</i> be cleared when a user logs on from the library to another.
	Y	The work area of the editor will be cleared automatically when a user logs on from the library to another.
PC download/ PC upload	Y	Modules contained in the library can be downloaded from the mainframe to a personal computer and uploaded from a personal computer to the mainframe respectively.
	N	Download and upload of modules will not be possible.
	This option only applies to mainframe computers; it has no effect under UNIX, OpenVMS and Windows.	
Close databases by logon	Y	All databases that have been accessed during the current Natural session will be closed automatically when a user logs on from the library to another.
	N	No databases will be closed when a user logs on from the library to another.
	When you set this option, you should also review the setting of the Natural profile parameter DBCLOSE.	

Security Limits

If you mark “Security Limits” in the Restrictions selection window with any character, the Security Limits window will be displayed. In this window, you can set the following limits:

Limit	Explanation
Non-activity logoff limit	<p>The maximum time (in seconds) which may elapse after the last terminal communication.</p> <p>If this time is exceeded, a new logon procedure will be invoked as soon as the next input is received from the terminal. Depending on the general option “Enable Error Transaction Before NAT1700/1701 Logoff”, the application's ON ERROR handling and/or error transaction may be processed before Natural Security performs the logoff.</p> <p>Possible values are 0 - 99999.</p>

Limit	Explanation
	If you wish no limit to be in effect, set this field to "0".
Maximum transaction duration	<p>The maximum time (in seconds) permitted for a single Adabas transaction. This feature can be used to prevent the blockage of resources for an excessive time. If the time is exceeded, the current transaction will be backed out.</p> <p>Possible values are 0 - 99999.</p> <p>If you wish no limit to be in effect, set this field to "0".</p> <p>The Natural system variable *TIME-OUT contains the time remaining before a time-out will occur. (The Adabas TT parameter (Adabas transaction time limit) will be checked separately).</p>
Maximum number of source lines	<p>The maximum number of source-code lines permitted for a user-written Natural program. If the line limit is exceeded, the Natural syntax checker will issue an appropriate error message.</p> <p>Possible values are 0 - 99999.</p>
Maximum amount of CPU time (MT)	<p>The maximum amount of CPU time (in seconds) to be used (as in the Natural profile parameter MT, described in the Natural <i>Parameter Reference</i> documentation).</p> <p>If you set this field to "0", the limit is determined by the value of the Natural profile parameter MT.</p> <p>If you wish the highest possible limit to be in effect, set this field to the maximum value (9999999).</p> <p>If you wish no limit to be in effect, set this field to "9999999999".</p> <p>This field only applies to mainframe computers; it has no effect under UNIX, OpenVMS and Windows.</p>
Maximum number of Adabas calls (MADIO)	<p>The maximum number of Adabas calls permitted between two screen I/O operations (as in the Natural profile parameter MADIO, described in the Natural <i>Parameter Reference</i> documentation). If the number specified is exceeded, the Natural program will be interrupted and an appropriate error message displayed.</p> <p>If you set this field to "0", the limit is determined by the value of the Natural profile parameter MADIO.</p> <p>If you wish the highest possible limit to be in effect, set this field to the maximum value (32767).</p> <p>If you wish no limit to be in effect, set this field to "99999".</p>
Maximum number of program calls (MAXCL)	<p>The maximum number of program calls permitted between two screen I/O operations (as in the Natural profile parameter MAXCL, described in the Natural <i>Parameter Reference</i> documentation). If the number specified is exceeded, the Natural program will be interrupted and an appropriate error message displayed.</p> <p>If you set this field to "0", the limit is determined by the value of the Natural profile parameter MAXCL.</p>

Limit	Explanation
	<p>If you wish the highest possible limit to be in effect, set this field to the maximum value (32767).</p> <p>If you wish no limit to be in effect, set this field to "99999".</p>
Processing loop limit (LT)	<p>The maximum number of records which may be read in any given processing loop of the library (as in the Natural profile parameter LT, described in the <i>Natural Parameter Reference</i> documentation).</p> <p>If you set this field to "0", the limit is determined by the value of the Natural profile parameter LT.</p> <p>If you wish the highest possible limit to be in effect, set this field to the maximum value (2147483647).</p> <p>If you wish no limit to be in effect, set this field to "9999999999".</p>

Session Parameters

If you mark "Session Parameters" in the Restrictions selection window with any character, the Session Parameters screen will be displayed.

On this screen, you can specify values for the following Natural session parameters, which will override the default parameter values set during Natural installation:

Parameter	Short Description
DC	Character for decimal point notation
CF	Character for terminal commands
CLEAR	Processing of CLEAR key in NEXT mode
IA	Input assign character
IM	Input mode
ID	Input delimiter character
SA	Sound terminal alarm
DU	Dump generation
EJ	Page eject
FS	Default format/length setting for user-defined variables
WH	Wait for record in hold status
ZD	Zero-division check
LS	Line size
PS	Page size for Natural reports
SL	Source line length (on mainframes only)
SF	Spacing factor

If a parameter value is blank (or "0" for a parameter which takes numeric values), the corresponding default value applies.

For information on the individual session/profile parameters, see the *Natural Parameter Reference* documentation.

Moreover the screen provides the following fields:

Field	Explanation
Adabas open (OPRB)	<p>You can specify the contents of the record buffer used with the Adabas OPEN command. If so, a restricted OPEN will be executed, which means that only files included in the record buffer may be referenced. If no record buffer contents are specified, all accessible files may be referenced (see also the <i>Adabas Command Reference</i> documentation).</p> <p>If this field is set to "NOOPEN", no Adabas OPEN command will be executed.</p> <p>If this field is left blank, an OPRB parameter specified dynamically when invoking Natural applies for this library (see the <i>Natural Parameter Reference</i> documentation for details on the profile parameter OPRB).</p>
Spool profile	<p>You can specify the name of the spool profile. This is only applicable if Natural Advanced Facilities is installed; see the <i>Natural Advanced Facilities</i> documentation for details.</p>
Adabas password	<p>You can specify the Adabas password used for access to the Adabas data files (not system files) referenced by the library. This is only relevant if the corresponding files are password-protected under Adabas Security.</p> <p>The password specified in the security profile applies to all database access statements for which neither an individual password is specified nor a <code>PASSW</code> statement applies. It applies within the library in whose security profile it is specified, and also remains in effect in other libraries you subsequently log on to and in whose security profiles no password is specified. See also the <code>PASSW</code> statement in the <i>Natural Statements</i> documentation.</p>
SLOCK	<p>This field applies on mainframes only; on other platforms, its setting will be ignored.</p> <p>This field controls source locking and determines how concurrent updates of Natural source members in the library are to be handled. Its possible values PRE, SPOD, POST and OFF corresponds to those of the Natural profile parameter SLOCK.</p> <p>If this field is left blank, the profile parameter SLOCK as set for the current Natural session applies for this library.</p> <p>See the <i>Natural Parameter Reference</i> documentation for details on the SLOCK parameter.</p>

Natural RPC Restrictions

When you press PF8 on the Session Parameters screen, another screen will be displayed in which you can set various restrictions that apply when subprograms contained in the library are executed by means of Natural RPC in a client/server environment.

Field	Explanation	
Expiration Criteria	<p>The following criteria determine how often / how long subprograms in the library can be executed by means of Natural RPC.</p> <p>When one of the criteria is reached, the criteria can be reset either by means of the Natural application programming interface USR1071 or by the user newly logging on to the library.</p>	
Use Count	<p>Determines how many times remote subprograms can be executed.</p> <p>A value of "0" means that no such limit is in effect.</p>	
Number of Days	<p>Determines for how many days remote subprograms can be executed.</p> <p>The days are counted beginning with the logon to the library.</p> <p>A value of "0" means that no such limit is in effect.</p>	
Number of Hours/Minutes	<p>Determines for how many hours/minutes remote subprograms can be executed.</p> <p>The time is counted beginning with the logon to the library.</p> <p>A value of "0" means that no such limit is in effect.</p>	
Allow Overwriting by User Exit USR1071	Y	The above expiration criteria in the library security profile, as well as the user ID and password from the client logon procedure, can be overwritten by criteria specified with the Natural application programming interface USR1071.
	N	No data can be set/overwritten by the Natural application programming interface USR1071.
Server Session Options:		
Close All Databases	This option allows you to control the logon-/logoff-dependent closing of databases. It affects all databases which have been opened by remote subprograms contained in the library:	
	N	The databases are <i>not</i> closed when a logon/logoff to/from the library is performed.
	Y	The databases are closed when a <i>logon</i> to the library is performed.
		If "Impersonation" is activated in the RPC server profile , "Y" has the same effect as "F" (see below).
	F	The databases are closed when a <i>logon</i> to the library is performed, and when a <i>logoff</i> from the library is performed.
This option is only relevant if the option LOGONRQ=ON is set in the Natural profile parameter RPC or NTRPC macro. If you wish to have one user-queue element per client		

Field	Explanation	
	session for each database accessed by the RPC server, it is recommended that you set LOGONRQ=ON and "Close All Databases" to "Y" or "F".	
Logon Option	This option determines which logon data are evaluated by Natural Security when the library is accessed via a Natural RPC service request:	
	N	Natural RPC user ID and password are evaluated. (*)
	E	Natural RPC user ID and password are evaluated. (*) In addition, it is checked if the Natural RPC user ID is identical to the EntireX user ID.
	A	Only the Natural RPC user ID is evaluated (similar to the Natural profile parameter AUTO=ON, but for this library only).
	S	Only the Natural RPC user ID is evaluated (similar to the Natural profile parameter AUTO=ON, but for this library only). In addition, it is checked if the Natural RPC user ID is identical to the EntireX user ID.
	(*) If impersonation is active for the Natural RPC server, the password is not evaluated (as this will be performed by an external security system). For details, see Validation of an RPC Service Request in the section <i>Protecting Natural RPC Servers and Services</i> .	
Logon Recorded	This option determines whether logons to the library are recorded when the library is accessed via Natural RPC service requests:	
	N	Logons to the library via Natural RPC service requests are not recorded.
	Y	Logons to the library via Natural RPC service requests are recorded. Every time a user accesses the library via a Natural RPC service request, a logon record will be written by Natural Security. You may review the activities of users by viewing these logon records (see Logon Records in the section <i>Administrator Services</i> for further information).
	L	The value of the option "Logon recorded" in the General Options section of the library profile determines whether logons to the library via Natural RPC service requests are to be recorded or not.
	*	The value of the option "Logon recorded" option in the Library And User Preset Values of Administrator Services determines whether logons to libraries via Natural RPC service requests are to be recorded or not.
Lock User Option	This option determines whether the Lock User feature is to be active when the library is accessed via Natural RPC service requests:	
	N	The Lock User feature is not active for access attempts to the library via Natural RPC service requests.

Field	Explanation	
	X	The Lock User feature is active for access attempts to the library via Natural RPC service requests. Once a user has reached the maximum number of logon attempts without supplying the correct password, he/she will be locked, that is, the user ID will be made “invalid”. Natural Security “remembers” unsuccessful attempts across sessions: The error counters for the client user IDs which were tried out unsuccessfully are kept for access attempts in subsequent sessions, thus reducing the number of subsequent attempts with these IDs. The error counter for a user ID is only reset after a successful logon.
	*	The value of the Lock User option in the security profile of the Natural RPC server determines whether or not the Lock User feature is active for access attempts to libraries on that server via Natural RPC service requests. See Components of a Server Profile in the section <i>Protecting Natural RPC Servers And Services</i> .
	For details on the Lock User feature, see also the Lock User Option in the General Options section of <i>Administrator Services</i> .	

The Natural application programming interfaces USR1071 and USR2071 mentioned above are contained in library SYSEXT.

For further information on Natural RPC with Natural Security, see the section **Protecting Natural RPC Servers and Services** in the Natural Security documentation, and the sections *Using Natural RPC With Natural Security* and *Logon To A Server Library* in the *Natural Remote Procedure Call* documentation.

Command Restrictions

If you mark “Command Restrictions” in the Restrictions selection window with any character, the Command Restrictions screen will be displayed. On this screen, you can allow or disallow the use of individual Natural system commands.

By default, all commands shown on the Command Restrictions screen are marked with “Y”, which means that all commands are allowed.

- Mark with “Y” each command you wish to be available for use in the library.
- Mark with “N” each command you wish *not* to be used in the library.

For the SCAN command, you can specify the following settings:

- “Y” - The command is allowed.
- “N” - The command is not allowed.
- “R” - The command is allowed; however, its Replace option is not allowed.

- “B” - The command is allowed; however, its Replace option is only allowed in batch mode (that is, if the Natural system variable *DEVICE is set to “BATCH”).
- “O” - The command is allowed; however, its Replace option is only allowed online (that is, if *DEVICE is set to any value other than “BATCH”).

For information on the individual commands, see the Natural *System Commands* documentation.

Those commands which are displayed intensified on the Command Restrictions screen use the Natural syntax checker and consequently Natural statements (which may also be allowed/disallowed individually; see [Statement Restrictions](#) below).

Restricting the Use of the SCAN Command

You can either disallow the system command SCAN altogether for a library via the Command Restrictions (as described above), or you can control its use via the Utilities option:

- If SCAN is marked with “N” on the Command Restrictions screen, the SCAN command cannot be used in the library (regardless of the Utilities option).
- If SCAN is marked with “Y” on the Command Restrictions screen, the [Utilities](#) option (in the General Options part of the library profile) determines who may use the SCAN command in the library. The Utilities option may take one of the following values:

N	No protection - The SCAN command may be used in the library by any user.
O	Permission for Owners - Only the owners of the library may use the SCAN command; if no owner is specified, any user of type ADMINISTRATOR may use it. In a private library in private mode, in addition to the owners, the user with the same ID as the library ID may use the SCAN command. In batch mode, please note that an owner who requires a countersignature from a co-owner cannot use the SCAN command (as countersignatures are not possible in batch mode).
P	Permission under Protection rules - The People/Terminal protection of the library applies: Only users who may use the library - and only under the conditions under which they may use it - may use the SCAN command. For a private library in private mode, the following applies: The user with the same ID as the library ID may use the SCAN command; anyone else may use it only after entering that user's password (on a countersignature screen provided for that purpose). In batch mode, please note that a user cannot use the SCAN command in another user's private library in private mode (as no password can be entered in batch mode).

UNIX Shell Commands

You can also allow or disallow the execution of UNIX shell commands from within a Natural program. These commands are executed from within a Natural program by invoking the Natural user exit SHCMD via the statement `CALL SHCMD` being issued by the program.

To allow/disallow the execution of shell commands from within a program in the library, you mark `CALL SHCMD` on the Command Restrictions screen as follows:

- Y = Shell commands can be executed.

- N = Shell commands *cannot* be executed.

Editing Restrictions

If you mark “Editing Restrictions” in the Restrictions selection window with any character, the Editing Restrictions window will be displayed. In this window, you may allow or disallow the editing of Natural objects of certain object types.

By default, all object types shown in the Editing Restrictions window are marked with “Y”, which means that objects of all types may be edited.

- Mark with "Y" each type of object whose editing you wish to be allowed in the library.
- Mark with "N" each type of object whose editing you wish *not* to be allowed in the library.

For information on Natural object types, see the *Natural Programming Guide*; for information on the Natural editors, see the *Natural Editors* documentation.

To disallow editing altogether, you may disallow the use of the EDIT command (see [Command Restrictions](#) above). When you disallow the EDIT command, all object types in the Editing Restrictions window are automatically marked with “N”. When you allow the EDIT command again, all object types in the Editing Restrictions window are automatically marked with “Y” again.

Statement Restrictions

If you mark “Statement Restrictions” in the Restrictions selection window with any character, the Statement Restrictions screen will be displayed. On this and the next screen, you may allow or disallow the use of individual Natural statements. To get from this screen to the next and back again, you press PF7 and PF8 respectively.

By default, all statements shown on the Statement Restrictions screen are marked with “Y”, which means that all statements are allowed.

- Mark with "Y" the Natural statements you wish to be allowed for use in the library.
- Mark with "N" the Natural statements you do *not* wish to be used in the library.

For the `FIND` statement and other database access statements, you may also allow/disallow individual clauses.

Any Natural statement which is not listed on the Statements Restrictions screen is always allowed (for example, the statement `END`).

The Statement Restrictions take effect when a programming object is syntax-checked at compilation.


Disallow/Allow Modules

With this option, you can restrict the use of modules (programming objects) in a library, that is, you can disallow/allow that they can be executed or invoked for execution.

This option may be evaluated differently on different platforms, depending on the option **Module Protection Mode**, as described in the section *Administrator Services*.

In the Restrictions selection window, besides the field you mark to select “Disallow/Allow Modules”, there is a second field, in which you can enter one of the following:

X	This causes all modules to be allowed; individual modules cannot be disallowed (the Disallow/Allow Modules screen will not be invoked). If you enter an "X", do not at the same time mark the selection field.
D	All modules are initially allowed, and you may disallow individual modules.
A	All modules are initially disallowed, and you may allow individual modules.

 **Note:** For the Display function, you can only mark the selection field; regardless of the setting of the second field, the Disallow/Allow Modules screen will be displayed showing the list of allowed/disallowed modules.

If you mark “Disallow/Allow Modules” in the Restrictions selection window with any character and enter a "D" or "A" in the second field, the Disallow Modules screen or Allow Modules screen respectively will be displayed:

```
11:13:46                *** Natural Security ***                2009-07-28
                        - Disallow Modules -
Library  SKYLIB
Module   T Status      Mark  Module   T Status      Mark
-----
#CADMIUM P ALLOWED      _  HELLO    P ALLOWED      _
#DANZA   P ALLOWED      _  HOTTA    P ALLOWED      _
#FIFO    P ALLOWED      _  MEHEECO  P ALLOWED      _
#GRACE   P ALLOWED      _  MOONROOF P ALLOWED      _
#PRESTO  P ALLOWED      _  SAHARA   P ALLOWED      _
#TEMPEST P ALLOWED      _  SCIPPIO  P ALLOWED      _
CALDANDO P ALLOWED      _  SKYLARK  P ALLOWED      _
CANNBALL P ALLOWED      _  WESTWAY  P ALLOWED      _
CARILLON P ALLOWED      _  WESTWIND N ALLOWED      _
ELCIELO  P ALLOWED      _  XANGO    M ALLOWED      _
***** Module Names held in User Buffer *****
_____
_____
-----
Reposition to .. _____ Display module names not held in UB .. _
```

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12---
 Help PrevM Exit AddOp Restr Flip - + Free Step1 Canc

Column T on the Disallow/Allow Modules screen indicates the object types of the modules:

P	Program
N	Subprogram
S	Subroutine
H	Helproutine
G	Global data area
L	Local data area
A	Parameter data area
M	Map
C	Copycode
3	Dialog
4	Class
7	Function
8	Adapter

On the Disallow/Allow Modules screen, mark with "D" the modules contained in the library you wish to be disallowed; mark with "A" the modules contained in the library you wish to be allowed. The first ten module names marked will be held in the user buffer.

In addition, the following subfunctions are available:

Module Names Held in User Buffer	<p>If you wish modules to be disallowed/allowed and their names to be held in the user buffer, type in their names into the ten fields provided on the Disallow/Allow Modules screen.</p> <p>If you type in a value followed by an asterisk (*), all module names beginning with that value will be disallowed/allowed and held in the user buffer.</p> <p>Those disallowed/allowed module names not held in the user buffer may be displayed by marking the "Display module names not held in User Buffer" field with any character. Unmark it to return to the Disallow/Allow Modules screen.</p> <p>If possible, the number of allowed/disallowed modules should not exceed 10; that is, all allowed/disallowed module names should be held in the user buffer; module names not held in the user buffer will cause a reduction in performance, as the Natural Security data file will have to be additionally accessed to check whether a module whose name is not held in the user buffer is allowed or not.</p>
---	---

Allowing/Disallowing "Non-Existent" Modules (PF9)	<p>The Disallow/Allow Modules screen of a library profile displays a list of all modules contained in the corresponding library. However, there may be modules which currently are not physically available (for example, because the corresponding database is not active, or the modules have not yet been written), and which would therefore not appear in the list of modules. Or in a heterogeneous production environment using a central mainframe FUSER system file, the library may exist not on the mainframe FUSER system file but in the file system on another platform. If you were to define a library profile for such a library, Natural Security on the mainframe computer would not know of that library, and the list of modules would therefore be empty.</p> <p>To enable you to disallow/allow such "non-existent" modules, the Allow/Disallow Modules function provides the subfunction "Free List of Modules". With this subfunction, you can predefine modules which are not physically present on the current FUSER system file.</p> <p>To invoke the subfunction, you press PF9 on the Disallow/Allow Modules screen. The "Free List of Modules" window will be displayed. In this window, you manually enter the names of modules and allow/disallow them.</p>
Steplibs (PF10)	<p>This subfunction does not apply on mainframe computers.</p> <p>With this subfunction, you can disallow/allow modules in the library's steplibs.</p> <p>To invoke the subfunction, you press PF10 on the Disallow/Allow Modules screen. A list of all the library's steplibs will be displayed. On the list, you select the library whose modules you wish to disallow/allow. Then, the list of modules contained in the selected steplib will be displayed, which you can then disallow/allow individually.</p> <p>When you disallow/allow modules in a steplib in this way, this does not mean you actually disallow/allow these modules in the library profile of the steplib. The steplib modules are only disallowed/allowed with respect to usage by the library whose profile you are currently maintaining (that is, the library from within whose library profile you have invoked the subfunction).</p>

Set Status of DDMs

This option only affects DDMs for which no security profiles have been defined. It allows you to set the status of all new DDMs to PUBLIC. On mainframes, this applies to the file status; on UNIX, OpenVMS and Windows, this applies to both the internal and the external status of DDMs.

In the Restrictions window, you can specify one of the following values for this option:

UNDF	The status of all DDMs without security profiles is undefined.
PUBL	The status of all DDMs without security profiles is PUBLIC.

By default, this option is set to “UNDF”, which means that DDMs for which no security profiles have been defined cannot be used.

If you set this option to “PUBL”, the status of all DDMs for which no security profiles have been defined is assumed to be PUBLIC, which means that these DDMs can be used. This allows you to use these DDMs without having to define security profiles for them.

For further information, see the sections [Protecting DDMs On Mainframes](#) and [Protecting DDMs On UNIX, OpenVMS and Windows](#).

Creating and Maintaining Library Profiles

This section describes the functions used to create and maintain library profiles. It covers the following topics:

- [Invoking Library Maintenance](#)
- [Adding a New Library](#)
- [Listing Undefined Libraries](#)
- [Selecting Existing Libraries for Processing](#)
- [Copying a Library](#)
- [Modifying a Library](#)
- [Renaming a Library](#)
- [Deleting a Library](#)
- [Displaying a Library](#)
- [Creating and Maintaining a Private Library](#)

Invoking Library Maintenance

On the Main Menu, enter code "M" for “Maintenance”. A window will be displayed.

In the window, mark object type “Library” with a character or with the cursor. The Library Maintenance selection list will be displayed.

From this selection list, you invoke all library maintenance functions as described below.

Adding a New Library

The Add Library function is used to define new libraries to Natural Security, that is, create library security profiles.



Note: To create library security profiles for system libraries of Natural and its subproducts more easily, you can use the Administrator Services function **“Definition of system libraries”**, which provides predefined security profiles for most system libraries.

▶ To add a new library security profile:

- 1 On the Library Maintenance selection list, enter the command ADD in the command line.
- 2 A window will appear, in which you enter a library ID and, optionally, the ID of a default profile:

Library ID	<p>Library IDs are used by Natural Security to identify libraries and their security profiles.</p> <p>A library ID may be 1 to 8 characters long, it must start with an upper-case alphabetical character, and it must be unique. It may consist of the following characters: upper-case alphabetical characters, numeric characters, hyphen (-) and underscore (_). It must not contain blanks.</p> <p>Before you start defining libraries, it may be advisable to conceive a logical system of library IDs that are related to the library names; this will help you to identify libraries more easily when maintaining them in Natural Security.</p>
Default Profile	<p>When you add a new library, you can either type in every item within the library security profile by hand; or you can use a pre-defined default library profile as the basis for the security profile you are creating.</p> <p>Before you use default library profiles, you should be familiar with the "normal" way of defining libraries (that is, without default profile).</p> <p>Default profiles are created and maintained in the Administrator Services subsystem.</p> <p>If you specify the ID of a default profile in the Add Library window, the items from the default profile will be copied into the library profile</p> <p>On the Add Library screen, you can overwrite the items copied from the default profile, and specify further items.</p> <p>For further information on default library profiles, see Library Default Profiles in the section <i>Administrator Services</i>.</p>

- 3 The Add Library screen will be displayed. On this screen, you may define a security profile for the library.

The Add Library screen and the subsequent screens/windows that may be part of a library security profile as well as the individual items you may define are described under *Components of a Library Profile* above.

When you add a new library, the owners specified in your own user security profile will automatically be copied into the library security profile you are creating.

Listing Undefined Libraries



Note: In a non-mainframe environment, the use of the SHOW command requires that work file 3 has been defined in your Natural parameter module, because internally the command uses the corresponding function of the Natural Object Handler utility.

An undefined library is a library which exists on the system file, but for which no library security profile has been created in Natural Security.

To ascertain which libraries are undefined, you can use the SHOW command. This will cause the to expand the Library Maintenance selection list to be expanded so that it also includes undefined libraries.

The syntax for the SHOW command is as follows:

```
SHOW ALL [FILE=(database-id,file-number,password,ciphercode)]
```

or

```
SHOW + [FILE=(database-id,file-number,password,ciphercode)]
```

With FILE you specify the system file whose undefined libraries are to be listed. If you omit the FILE specification, the undefined libraries on the current FUSER file will be listed.

The system file to which the expanded list of libraries refers is shown at the top of the Library Maintenance selection list. The Message column of the selection list indicates which of the listed libraries are undefined.

Instead of entering the SHOW ALL command (without FILE specification) in the command line of the Library Maintenance selection list, you can also press PF16.

If you want to list only the undefined libraries, you either enter the command SHOW UNDF (with or without FILE specification) in the command line, or enter "UNDF" in the protection status field (Prot.).

To revert the Library Maintenance selection list to the standard display of only defined libraries, you press PF16 again or enter the following command in the command line:

```
SHOW -
```



Note: To list undefined libraries, you can also use the application programming interface **NSCXR** (with object-type code "SF" (system file)).

► **To create a security profile for one undefined library:**

- 1 On the Library Maintenance selection list, you mark the library with function code "AD" or "AP".
- 2 With "AP", a window will appear, in which you can specify the ID of a **default profile** (see above). With "AD", this window will be skipped and no default profile used.
- 3 The Add Library screen will be displayed - as with Step 3 above.

► **To create security profiles for multiple undefined libraries:**

- On the Library Maintenance selection list, you either mark each of the libraries with function code "AD" or "AP"; or you press PF10 to simultaneously select all undefined libraries on the currently displayed page of the Library Maintenance selection list (corresponds to marking them all with "AP").

Steps 2 and 3 will then be repeated for one of the marked/selected libraries after another.



Note: To define undefined libraries, you can also use the Administrator Services function **Definition of Undefined Libraries**.

Selecting Existing Libraries for Processing

When you invoke Library Maintenance, a list of all libraries that have been defined to Natural Security will be displayed.

If you do not wish to get a list of all existing libraries but would like only certain libraries to be listed, you may use the Start Value and Type/Status options as described in the section **Finding Your Way In Natural Security**.

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed. In the window, mark object type "Library" with a character or with the cursor (and, if desired, type in a start value and/or protection status). The Library Maintenance selection list will be displayed:

12:47:45		*** NATURAL SECURITY ***		2009-07-31	
		- Library Maintenance -			
Co	Library ID	Library Name	Prot.	Message	
—	KETEST		YN		
—	KEX	TEST APPL-KE	YN		
—	KE1	KETEST	NN		

—	KJH	NN
—	KK-APPL	NN
—	KKAPP	NN
—	KKAPPC	NN
—	KKAPP1	NN
—	KKAPP2	NN
—	KKAPP3	NN
—	KKAPP4	YN
—	KKAPP7	NN
—	KKITEST	NN
—	KKPAC	NN
—	KKPROD	NN
Command ==>		
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---		
Help Exit Flip - + Canc		

For each library, the ID, name and protection status are displayed.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#). The list can be expanded to also include undefined libraries, as described under [Listing Undefined Libraries](#) above.

The following library maintenance functions are available (possible code abbreviations are underlined):

Code	Function
AD	Add library without default profile (only possible if the selection list has been expanded; see Listing Undefined Libraries above)
AP	Add library, optionally with default profile (only possible if the selection list has been expanded; see Listing Undefined Libraries above)
<u>C</u> O	Copy library
<u>M</u> O	Modify library
RE	Rename library
DE	Delete library
<u>D</u> I	Display library
LU	Link users to library
LF	Link library to files (this function is only available on mainframe computers)
MD	Modify DDM restrictions in library (this function is only available on UNIX, OpenVMS and Windows)
EP	Protect environments

To invoke a function for a library, mark the library with the appropriate function code in column “Co”.

You may select various libraries for various functions at the same time; that is, you can mark several libraries on the screen with a function code. For each library marked, the appropriate processing screen will be displayed. You may then perform for one library after another the selected functions.

Copying a Library

The Copy Library function is used to define a new library to Natural Security by creating a security profile which is identical to an existing library security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - *except* the owners (these will be copied from your own user security profile into the new library security profile you are creating).

In addition to duplicating a library profile, you can choose to also copy its links and utility profiles, as well as the actual library itself; this depends on the options described below.

How to Copy

On the Library Maintenance selection list, mark the library whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, specify the following:

To library	Enter the ID of the "new" library.
Library name	This field shows the name of the existing library. Overwrite it with the name of the "new" library.
With links	Enter "Y" or "N". With this option, you can, in addition to the library profile, also copy its links and utility profiles; see below for details.
With Natural objects	Enter "Y" or "N". With this option, you can duplicate the actual library itself. This means that a new library will be created on the FUSER system file, and all Natural programming objects contained in the existing library will be copied into this new library. (Internally this option uses the MAINUSER application programming interface of the Natural utility SYSMAIN.)

The Copy Library screen will be displayed, showing the new library security profile.

The individual components of the security profile you may define or modify are described under [Components of a Library Profile](#) above.

With Links

If you leave the “N” in the “with links” field of the Copy Library window:

- any links defined for the existing library will not apply to the new library;
- any library-specific and user-library-specific utility profiles for the existing library will not apply to the new library.

If you enter a “Y” in the “with links” field of the Copy Library window:

- any links that exist for the existing library are copied for the new library, and you have the option to cancel the links you wish not to apply to the new library;
- any library-specific and user-library specific utility profiles that exist for the existing library are copied for the new library.

The procedure is as follows:

1. Once you have made any changes to the copied security profile and then leave the Copy Library screen by pressing PF3, a list of users is displayed: it contains all users which are linked to the existing library.
2. On the list, you may mark individual users with “CL” to cancel any links you wish *not* to apply to the new library; all users you do not mark will automatically be linked to the new library in the same manner - normal or special link - as the existing library.
3. Once you have established all user links and leave the list of users by pressing PF3, a list of files is displayed: the list contains all files/DDMs to which the existing library is linked.
4. On the list, you may mark individual files/DDMs with “CL” to cancel any links you wish *not* to apply to the new library; to all files/DDMs you do not mark the new library will automatically be linked in the same manner - read or update link - as the existing library.

Modifying a Library

The Modify Library function is used to change an existing library security profile.

On the Library Maintenance selection list, you mark the library whose security profile you wish to change with function code “MO”. The security profile of the selected library will be displayed.

The individual components of the security profile you may define or modify are described under *Components of a Library Profile* above.

Renaming a Library

The Rename Library function allows you to change the library ID of an existing library security profile.

On the Library Maintenance selection list, you mark the library whose ID you wish to change with function code “RE”.

A window will be displayed in which you can enter a new ID for the library (and, optionally, change its name).

Depending on the setting of the general option “Deletion of non-empty libraries allowed” (as explained in the section *Administrator Services*), it may not be possible to rename a library security profile if the library contains any sources or object modules.

With Natural Objects

When you rename a library profile, this option allows you to also change the name of the actual library. This means that the library will be renamed on the FUSER system file, and all Natural programming objects contained in the library will be stored under the new library name. (Internally this option uses the MAINUSER application programming interface of the Natural utility SYS-MAIN.)

Deleting a Library

The Delete Library function is used to delete an existing library security profile.

On the Library Maintenance selection list, you mark the library you wish to delete with function code “DE”. A window will be displayed.

- If you have invoked the Delete Library function and should then decide against deleting the given library security profile, leave the Delete Library window by pressing `ENTER` without having typed in anything.
- If you wish to delete the given library security profile, enter the library's ID in the window to confirm the deletion.

When you delete a library, all existing links to the library will also be deleted.

Depending on the setting of the general option **“Deletion of Non-empty Libraries Allowed”** (described in the section *Administrator Services*), it may not be possible to delete a library security profile if the library still contains any sources or object modules.

If you mark more than one library with “DE”, a window will appear in which you are asked whether you wish to confirm the deletion of each library security profile by entering the library's ID, or whether all libraries selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a library accidentally.

With Natural Objects

When you delete a library profile, this option allows you to also delete the actual library itself. This means that the library - and all Natural programming objects it contains - will be deleted from the FUSER system file. (Internally this option uses the MAINUSER application programming interface of the Natural utility SYSMAIN.)

Displaying a Library

The Display Library function is used to display an existing library security profile.

On the Library Maintenance selection list, you mark the library whose security profile you wish to view with function code "DI". The security profile of the selected library will be displayed.

The individual components of the security profile are described under *Components of a Library Profile* above.

Creating and Maintaining a Private Library

Defining a Private Library

To define a private library to Natural Security, first mark the "Private Library" field in the user's security profile with "Y" (on the Add User, Copy User or Modify User screen) (marking this field does not cause any default private library profile to be created).

In the Additional Options window, you then select "Private Library"; or you press PF5 on the main user profile screen.

A Private Library screen will be displayed; the screen is identical to a "normal" library security profile screen (except when private libraries are used in private mode, in which case the screen does not contain the fields "People-protected" and "Terminal-protected"). On this screen and the subsequent screens/windows you define the security profile for the private library.

The library ID by which a private library is defined to Natural Security is identical to the respective user ID.

Maintaining a Private Library

In private mode, maintenance of existing private library profiles is performed via *User Maintenance*.

In public mode, private libraries also appear on the Library Maintenance selection list along with the other libraries, that is, they can be maintained like "normal" libraries with the library maintenance functions described above.

Deleting a Private Library

If private libraries are used in public mode, you delete a private library like any other library (see [Deleting a Library](#) above).

If private libraries are used in private mode, you delete a private library by marking the "Private Library" field in the user's security profile with "N". A window will be invoked in which you confirm the deletion by typing in the library ID.

Depending on the setting of the general option **"Deletion of Non-empty Libraries Allowed"** (described in the section *Administrator Services*), it may not be possible to delete a private library if it still contains any source or object modules.

9

Protecting Libraries

■ Protected Libraries	156
■ Linking Users to Libraries	158
■ Which Conditions of Use are in Effect?	162

This section describes how to control the access of users to protected libraries. It covers the following topics:

Protected Libraries

A library may be protected by specifying the values of “People-protected” and “Terminal-protected” in the **General Options** column of the library’s security profile.

Protection Combinations

The possible combinations of “People-protected” and “Terminal-protected” are listed below:

Protection	Explanation
People: N Terminal: N	The library is not protected. It may be used by any person from any terminal. The terminal need not be defined to Natural Security. The user must be defined to Natural Security. The user ID must be entered on the logon screen in order to be able to log on to the library.
People: L Terminal: N	This is identical to the above combination - with the following addition: Although the library is not protected, it is possible to link a group to the library. Only one group can be linked to the library, and the link must be a special link. This special link only applies to users of type “A” contained in the group. This feature is only intended to allow administrators different access to an unprotected library for maintenance purposes. (The special link to such a library can only be established via the function “Link users to library” which is invoked from the Library Maintenance selection list.) Note: When an administrator processes the library’s contents with a Natural utility under a condition under which the Utilities option in the library profile would apply, Natural Security will react as if this option were set to “N”.
People: Y Terminal: N	The library may be used only by persons who are linked to the library or are in a group that is linked to the library. It may be used from any terminal. The terminal need not be defined to Natural Security. The user (and the group if need be) must be defined to Natural Security. The user ID must be entered on the logon screen in order to be able to log on to the library.
People: N Terminal: Y	The library may be used by any person, but it may only be used from a terminal which is defined to Natural Security and is contained in a group which is linked to the library. No user ID is required on the logon screen to log on to the library.
People: Y Terminal: Y	The library may be used either by people linked to the library or from a terminal which is contained in a group which is linked to the library. In other words, by entering his or her user ID on the logon screen, a linked person may use the library from any terminal; people who are not linked to the library may only use the library from a linked terminal.
People: Y Terminal: A	The library may be used only by people from linked terminals: The person must be defined to Natural Security and must be in a group which is linked to the library (or may be linked directly, if user type “A” or “P”); the terminal must also be defined to Natural Security, and it must be contained in a group which is linked to the library. The user ID and library ID must be entered on the logon screen in order to be able to log on to the library.

Protection	Explanation
People: P Terminal: N	This combination only applies to private libraries in public mode. The user with the same ID as the library ID may use the library without requiring a link to it. Otherwise, this combination is identical to “People: Y, Terminal: N” (see above).
People: P Terminal: Y	This combination only applies to private libraries in public mode. The user with the same ID as the library ID may use the library without requiring a link to it. Otherwise, this combination is identical to “People: Y, Terminal: Y” (see above).
People: P Terminal: A	This combination only applies to private libraries in public mode. The user with the same ID as the library ID may use the library without requiring a link to it. Otherwise, this combination is identical to “People: Y, Terminal: A” (see above).
People: N Terminal: A	This combination is not possible!
People: L Terminal: Y	This combination is not possible!
People: L Terminal: A	This combination is not possible!

Changing a Protection Combination

Please take care when you alter an existing combination of “People-protected” and “Terminal-protected”. If the alteration results in a “lower” protection level, certain links will automatically be cancelled by Natural Security according to the following rules:

Change from	to	Effect on Links
any protection combination	People: N Terminal: N	All existing links to the library will be cancelled.
any protection combination	People: N Terminal: Y	All direct links of ADMINISTRATORS and PERSONs will be cancelled; links of GROUPs to the library will remain.
any protection combination	People: Y Terminal: N	No links will be cancelled.
any protection combination	People: Y Terminal: Y	No links will be cancelled.
People: N Terminal: Y	People: Y Terminal: Y	No links will be cancelled. However, all people contained in GROUPs which are linked to the library may now also log on the library!

Protecting a Private Library

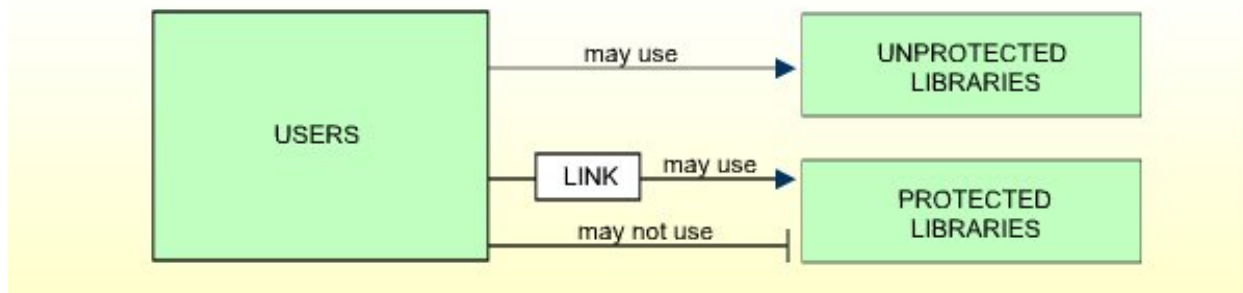
The user with the same user ID as the library ID always has access to his/her **private library**.

In public mode, other users' access to someone's private library is determined by the settings of the fields "People-protected" and "Terminal-protected" in the security profile of the private library. Possible values for the field "People-protected" are "P" (which is the default value, and which corresponds to "Y" in other library profiles) and "N" (which is the same as in other library profiles). Possible values for the field "Terminal-protected" are the same as for other libraries (Y, N or A). The possible protection combinations are described above.

In private mode, no other user has access to someone else's private library.

Linking Users to Libraries

To allow a user access to a protected library, a *link* has to be established between the user and the library.



Only users of types ADMINISTRATOR, PERSON, and GROUP can be linked to a library.

Users of types ADMINISTRATOR and PERSON can be linked to a library either directly or via a GROUP.

Users of types MEMBER and TERMINAL can be linked to a library only via a GROUP; that is, they must be assigned to a GROUP, and the GROUP be linked to the library.

Two functions are available to establish and maintain links between users and libraries:

- To link *one user* to *various libraries*, you use the function "Link user to libraries" (which is invoked from the User Maintenance selection list).
- To link *various users* to *one library*, you use the function "Link users to library" (which is invoked from the Library Maintenance selection list).

Both functions are described below.

Linking a Single User to Libraries

The function “Link user to libraries” is used to link one user to one or more libraries.

On the User Maintenance selection list, you mark the user you wish to link with function code “LL”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a Start Value (as described in the section [Finding Your Way in Natural Security](#)) for the list of libraries to be displayed.
- **Selection criterion** - N = none: all libraries will be listed; L = linked: only libraries to which the user is already linked (normal and special links, including temporarily locked ones) will be listed; U = unlinked: only libraries to which the user is not yet linked will be listed.

Then, the Link User To Libraries selection list will be displayed, showing the list of libraries.

The list includes all protected libraries; that is, if you link a user of type PERSON or ADMINISTRATOR, the list includes all libraries with “People-protected” set to “Y”; if you link a user of type GROUP, the list includes all libraries with at least one of the two protection values set to “Y”.

The list can be scrolled as described in the section [Finding Your Way in Natural Security](#).

On the list, you mark the libraries to which you wish to link the given user.

In the “Co” column, you may mark each library with one of the following function codes (possible code abbreviations are underlined):

Code	Function
LK	Link - The user may use the library with the security profile of the library being in effect.
SL	Special Link - The user may use the library with a special security profile to be defined for the link; the link profile will take precedence over the library profile. For details on special links, see Special Links below.
CL	Cancel - An existing link or special link will be cancelled.
TL	Temporarily Locked - An existing link or special link will be suspended until it is re-established. A suspended link or special link can be re-established by marking the library concerned with “LK” or “SL” again. When a special link is re-established, the original link security profile will be re-established, too.
DL	Display Special Link - The security profile of an existing special link between the user and the library will be displayed.
<u>D</u> I	Display Library - The security profile of the library will be displayed.
LD	Modify DDM Restrictions in Special Link Profile (This function is not available on mainframe computers. It corresponds to function “MD” as described under Creating And Maintaining DDM Profiles in the section <i>Protecting DDMs On UNIX, OpenVMS and Windows</i>).

You can mark one or more libraries on the screen with a function code. For each library marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect for each library.

Linking Multiple Users to a Library

The function “Link user to libraries” is used to link one or more users to one library.

On the Library Maintenance selection list, you mark the library to which you wish to link users with code “LU”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a Start Value (as described in the section [Finding Your Way in Natural Security](#)) for the list of users to be displayed.
- **Selection criterion** - N = none: all users will be listed; L = linked: only users which are already linked to the library (normal and special links, including temporarily locked ones) will be listed; U = unlinked: only user which are not yet linked to the library will be listed.

Then, the Link Users To Library selection list will be displayed, showing the list of users.

The list includes all users of types GROUP, ADMINISTRATOR, and PERSON.

The list can be scrolled as described in the section [Finding Your Way in Natural Security](#).

On the list, you mark the users you wish to be linked to the given library.

In the “Co” column, you may mark each user with one of the following function codes (possible code abbreviations are underlined):

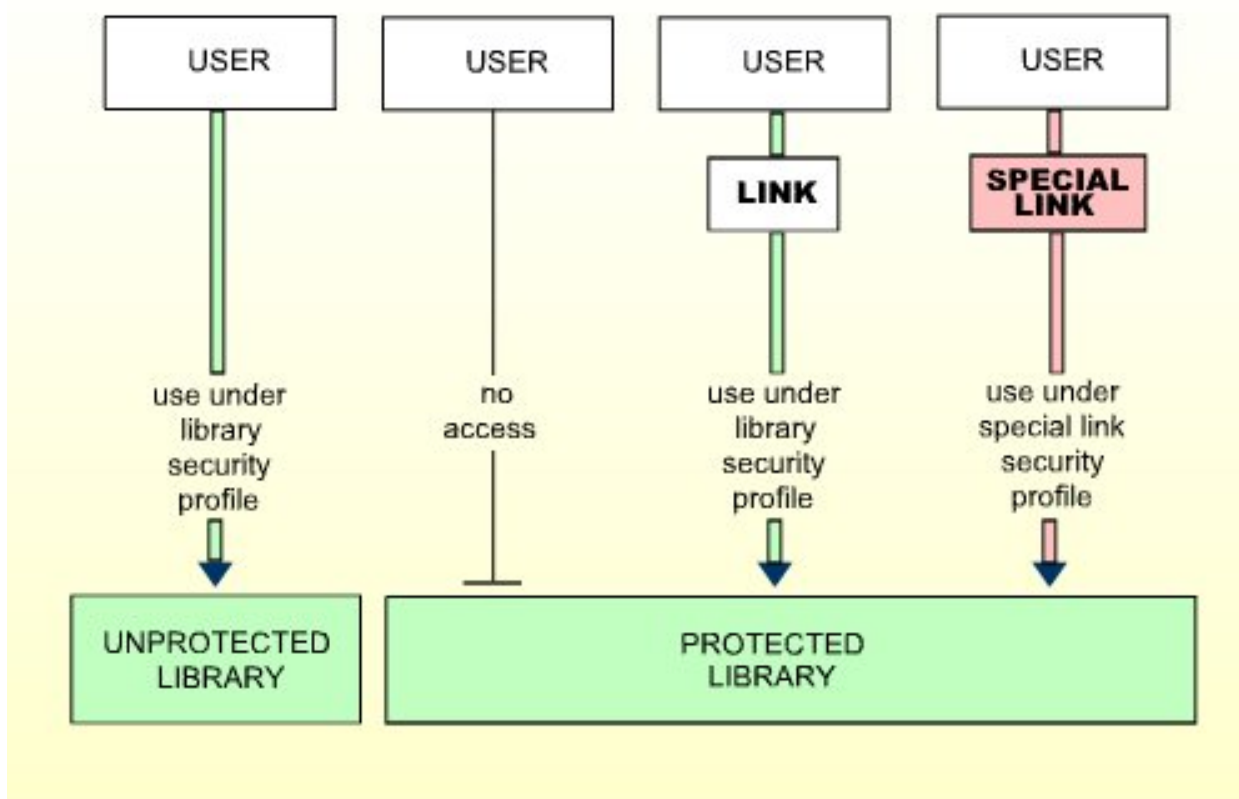
Code	Function
LK	Link - The user may use the library with the security profile defined for the library being in effect.
SL	Special Link - The user may use the library with a special security profile to be defined for the link; the link profile will take precedence over the library profile. For details on special links, see Special Links below.
CL	Cancel - An existing link or special link will be cancelled.
TL	Temporarily Locked - An existing link or special link will be suspended until it is re-established. A suspended link or special link can be re-established by marking the user concerned with “LK” or “SL” again. When a special link is re-established, the original link security profile will be re-established, too.
DL	Display Special Link - The security profile of an existing special link between the user and the library will be displayed.
<u>D</u> I	Display User - The security profile of the user will be displayed.

Code	Function
LD	Modify DDM Restrictions in Special Link Profile (This function is not available on mainframe computers. It corresponds to function “MD” as described under Creating And Maintaining DDM Profiles in the section <i>Protecting DDMs On UNIX, OpenVMS And Windows</i>).

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect for each user.

Special Links

If a library security profile determines the conditions under which the library may be used generally, the special link security profile determines the conditions under which the user (or group of users) thus linked may use the library. This means that by using special links you may define for different users different conditions of use of the same library.



Creating a Special Link

If you mark a user/library with “SL”, you may define the security profile for this Special Link on the screens which will be displayed. The default settings which will appear on the Special Link security profile screens are taken from the security profile of the library.

The items you may define as part of a Special Link security profile correspond with the items you may define as part of a library security profile (see [Components of a Library Profile](#) in the section *Library Maintenance*).

Modifying a Special Link

To modify an existing Special Link security profile, mark the respective user/library with “SL” again on the Link Users To Library or Link User To Libraries screen: the Special Link security profile screen will then be invoked for modification.

Displaying a Special Link

To view the security profile of a Special Link, mark the respective user/library with “DL” on the Link Users To Library or Link User To Libraries screen: the Special Link security profile screen will then be displayed.

Which Conditions of Use are in Effect?

When a user logs on to a protected library, Natural Security will execute a number of checks to determine under which conditions the user may use the library. If none of the checks are positive, the logon will be rejected.

The following checks will be executed in the following order:

Library Protection		Checks Performed
1.		First: Check whether the user is linked directly to the library; if the user is linked with a special link, the conditions defined in the special link security profile will be in effect; if the user is linked with an ordinary link, the conditions defined in the library security profile will be in effect. Second: Check whether the user is in a group which is linked to the library; if the user is contained in more than one group, these groups will be checked in the following order: first the “privileged groups” in the user's security profile will be checked in order of entry, then the other groups will be checked in alphabetical order; the first linked group found will be selected; if the group is linked with a special link, the conditions defined in the special link security profile will be in effect; if the group is linked with an ordinary link, the conditions defined in the library security profile will be in effect.
People:	Y	
Terminal:	N	

Library Protection		Checks Performed
2.		Check whether the terminal is in a group which is linked to the library; if the terminal is contained in more than one group, these groups will be checked in the following order: first the “privileged groups” in the terminal's security profile will be checked in order of entry, then the other groups will be checked in alphabetical order; the first linked group found will be selected; if that group is linked with a special link, the conditions defined in the special link security profile will be in effect; if that group is linked with an ordinary link, the conditions defined in the library security profiles will be in effect.
People:	N	
Terminal:	Y	
3.		If the user logs on <i>with a user ID</i> , the same checks as under 1. will be executed. If the user logs on <i>without specifying a user ID</i> , the same checks as under 2. will be executed.
People:	Y	
Terminal:	Y	
4.		The same checks as under 1. will be executed.
People:	Y	
Terminal:	A	



Note: The terminal must be in a group which is linked to the library, but the conditions of use are determined by the user's link.

PROFILE Command

When logged on to a library, a user may enter the Natural system command PROFILE to ascertain which conditions of use are currently in effect.

When you enter the PROFILE command, the Security Profile screen is displayed, showing the following information:

User	
ID	The user's ID.
Name	The user's name.
Type	The user type.
Link ID	The current value of the Natural system variable *GROUP. An asterisk (*) next to the ID indicates that the group's/user's link to the current library is a Special Link.
ETID	The current value of the Natural system variable *ETID.
Library	
ID	The ID of the current library.
Name	The name of the current library.
Steplibs	The steplibs of the current library.
Transactions	
Startup	The current value of the Natural system variable *STARTUP.

User	
Restart	The name of the restart transaction.
Error	The current value of the Natural system variable *ERROR-TA.

Additional Options

If you mark the field "Additional Options" on the Security Profile screen with "Y" or press PF4, a window will be displayed from which you can select the following items of information:

- Security options
- Security limits
- Session parameters
- Command restrictions
- Editing restrictions
- Statement restrictions
- Time windows
- System files
- Natural version

The options where something is defined for the current user are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window/screen will be displayed (in the order of the items in the selection window).

Utility Access Rights

If you press PF5, the NSC Utility Access Rights window will be displayed, providing an overview of the utility functions which you are allowed to use in each library.

- If you have issued the PROFILE command from within a utility, the window lists the functions available in that utility.
- If you have issued the PROFILE command elsewhere, the window lists all utilities along with information on whether some or all functions of a utility are allowed/disallowed for a specific library. (The notation <others> in the Library field of the window indicates all libraries for which nothing specific has been defined.) To obtain more detailed information on the utility functions allowed for a particular library, you can select one or more libraries from the window by marking them with any character.

10

Protecting Environments

■ Concept of Environment Protection	166
■ Activation of Environment Protection	166
■ Defining Environment Profiles	167
■ Components of an Environment Profile	168
■ Disallowing/Allowing Access to Libraries in Environments	171
■ Disallowing/Allowing Users Access to Environments	173

This section covers the following topics:

Concept of Environment Protection

Natural Security allows you to make users' access to a library environment-specific. A Natural *environment* is determined by the combination of the system files FNAT, FUSER, FSEC and FDIC. You define a security profile for each environment (that is, for each system-file combination) you wish to protect, and control users' access to it. You can also make a library accessible in some environments, but not in others.

A logon to another environment occurs when a users logs onto a library located on another FUSER system file (as specified by the **“Library File”** DBID/FNR in the library profile).

Whenever a user logs on to a library in another environment, Natural Security will check whether:

- access to the library is allowed in that environment, and
- the user is authorized to access that environment.

Such a check is performed not only when a user explicitly logs on to a library, but also when the user invokes a function which implicitly accesses another library or processes the contents of another library.

Activation of Environment Protection

Environment protection is activated by setting the general option **“Environment Protection”** to **“Y”**.

If environment protection is active, the following applies:

- Access to undefined environments is not possible.
- For every environment to be accessed, an environment security profile has to be defined.
- By default, access to a library is allowed in any defined environment.
- By default, access to a defined environment is allowed for all users.
- For individual defined environments, you can disallow access to a library.
- For individual users, you can disallow access to a defined environment.

To deactivate environment protection, you set the general option **“Environment Protection”** option to **“N”**.

Defining Environment Profiles

The Administrator Services function “Environment Profiles” is used to define environment profiles, that is, security profiles for the individual system-file combinations.

To invoke this function, you select “Administrator Services” on the Main Menu. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (as explained in the section *Administrator Services*).

On the Administrator Services Menu 2, you select “Environment profiles”. The Environment Maintenance selection list will be invoked.

Environment Maintenance Selection List

The Environment Maintenance selection list displays a list of all environment profiles which have been defined.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

For each environment profile, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed.

Protection Status

The protection status can be:

I	The environment profile is inactive (both NSC Protection = N and NSF Protection = N in the environment profile).
N	Access to the environment is evaluated by Natural Security (NSC Protection = Y in the environment profile).
S	Access to the environment is evaluated by the SAF server (NSF Protection = Y in the environment profile).

Available Functions

The following functions are available:

Code	Function
AD	Add a new environment profile. (You can also invoke this function by entering "AD" in the Command line.)
CO	Copy environment profile.
MO	Modify environment profile.
RE	Rename environment profile.
DE	Delete environment profile.
DI	Display environment profile.
EP	Protect environment.

To invoke a function for an environment, you mark the environment with the appropriate function code in column "Co".

You may select various environments for various functions at the same time; that is, you can mark several environments on the screen with a function code. For each environment marked, the selected functions will then be executed one after another.

Components of an Environment Profile

When you add a new environment or modify an existing one, the Define Environment Profile screen will be displayed. The items you can define as part of an environment profile on this screen and any subsequent screens/windows are:

Field	Explanation
Environment ID	You specify a descriptive name for the environment profile.
Alias	<p>You can specify a one-character alias for the environment profile. An alias can be shared by multiple environment profiles. By specifying the same alias in several environment profiles, you can form groups of environments.</p> <p>For example, you can use aliases like: D - for all development environments, T - for all test environments, P - for all production environments.</p> <p>This will make the maintenance of environment profiles easier, because you can use the alias as selection criterion on the Environment Maintenance selection list to list all profiles which have the same alias.</p>

Field	Explanation
	For Natural SAF Security the following applies: The alias is used in the external security system to define the resources related to the system-file combination of this environment. The rules defined for an alias in the external security system apply to all system-file combinations in whose environment profiles this alias is specified.
General Options	<p>You specify by which system the environment is to be protected:</p> <ul style="list-style-type: none"> ■ NSC Protection: If set to "Y", this activates the environment for validation by Natural Security, as described in this documentation. ■ NSF Protection: If set to "Y", this activates the environment for validation by the SAF server, as described in the <i>Natural SAF Security</i> documentation. This validation requires that the option "Protect Environment" in the General NSF Options is set to "Y" (see <i>Natural SAF Security</i> documentation). <p>If both are set to "N", the environment profile is not active, that is, it is treated as if it were not defined.</p>
System Files	<p>You define the environment by specifying the database IDs and file number of each system file (FUSER, FDIC, FSEC, FNAT). This combination of system files identifies the environment, and must be unique.</p> <p>Once entered, the values of these fields cannot be changed.</p> <p>If you press PF9 on the main environment profile screen, a window will be displayed showing the system-file combination of your current Natural session. In the window, you can mark with any character the system files you wish to be part of the environment whose profile you are creating.</p>

Additional Options

If you either mark the field "Additional Options" with "Y" or press PF4, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners
- Session Options

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this environment security profile or allow/disallow users' access to it. If no owner is specified, any user of type ADMINISTRATOR may do so.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance/link permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures.</p>
Session Options	See below.

Session Options

Option	Explanation
TEST Command	<p>With this option, you can control the use of the Natural system command TEST in the environment. Possible values are:</p> <ul style="list-style-type: none"> ■ Y = The TEST command can be used without any restrictions. ■ P = The TEST command can be used with the following restrictions: the debugger commands <code>MODIFY VARIABLE</code>, <code>ESCAPE ROUTINE</code>, <code>ESCAPE BOTTOM</code> and <code>STOP</code> cannot be used. ■ N = The use of the TEST command is disallowed altogether. <p>This option only applies to environments on mainframe computers.</p>

Disallowing/Allowing Access to Libraries in Environments

By default, when environment protection is active, access to a library is allowed in any environment. For individual environments, you can disallow access to a library.

When access to a library is disallowed in at least one environment, the fact that the library is “environment-protected” will be indicated in the library’s security profile.

Two functions are available to disallow/allow environment-specific access to libraries:

- To disallow/allow access to various libraries for one environment, you use the function **“Protect environment”** (which is invoked from the Environment Maintenance selection list).
- To disallow/allow access to one library for various environments, you use the function **“Protect environments”** (which is invoked from the Library Maintenance selection list).

Both functions are described below.

Protecting a Single Environment for Multiple Libraries

On the Environment Maintenance selection list, you mark the environment you wish to protect with “EP”.

A window will be displayed. Here you enter an “L” in the field “Protect for users/libraries”. You can also enter a Start Value (as described in the section *Finding Your Way in Natural Security*) for the list of libraries to be displayed. In addition, you can select the option “Select only disallowed ones” - in which case the list of libraries to be displayed will only include those libraries for which access in the environment is currently disallowed.

Then, the Disallow/Allow Libraries screen will be displayed, showing the list of libraries. The list can be scrolled as described in the section *Finding Your Way In Natural Security*.

On the list, you mark the libraries for which you wish to disallow/allow access in the environment.

In the “Co” column, you may mark each library with one of the following function codes:

Code	Function
ED	Disallow - The library cannot be accessed in that environment.
EA	Allow - The library can be accessed in that environment.

You can mark one or more libraries on the screen with a function code. For each library marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each library.

Protecting Multiple Environments for a Single Library

On the Library Maintenance selection list, you mark the library for which you wish to with function code “EP”.

A window will be displayed, in which you have the following options:

Option	Explanation	
Disallow/allow	D	Access to the library is initially allowed for all environments, and you can disallow it for individual ones.
	A	Access to the library is initially disallowed for all environments, and you can allow it for individual ones.
	When you later invoke this function and change the value of this option, the “allowed/disallowed” status of all environments will be changed for this library.	
Sorted by environment ID / Sorted by alias	By marking one of these two fields with a character, you can choose to have the list of environments to be displayed sorted by environment IDs or by aliases. The latter allows you to simultaneously allow/disallow access for all environments which have the same alias (see below).	
Start value	In one of these two fields, you can enter a start value (as described in the section Finding Your Way in Natural Security) for the list of environments to be displayed. Depending on how the list is to be sorted, you can specify either the database ID / file number of the environments' FNAT system file or a one-character alias as start value.	
Select only disallowed/allowed ones	If you select this option, the list of environments to be displayed will only include - depending on the above option “Disallow/allow” - either those for which access is allowed or those for which it is disallowed.	

Then, the Disallow/Allow Environments screen will be displayed, showing the list of environments. For each environment, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed. The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

On the list, you mark the environments for which you wish disallow/allow access to the library.

In the “Co” column, you may mark each environment with one of the following function codes:

Code	Function
ED	Disallow - The library cannot be accessed in that environment.
EA	Allow - The library can be accessed in that environment.

You can mark one or more environments with a function code. For each environment marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each environment.

If the list is sorted by alias, you do not mark individual environments. Instead, you mark an alias, and the selected function will be applied to all environments which have that alias.

Disallowing/Allowing Users Access to Environments

By default, when environment protection is active, access to an environment is allowed for all users. For individual users you can disallow access to an environment.

Access to an environment can only be allowed/disallowed for users of types GROUP, ADMINISTRATOR and PERSON. For users of types ADMINISTRATOR and PERSON it can be allowed/disallowed either directly or via a GROUP. For users of types MEMBER and TERMINAL, it can only be allowed/disallowed for the GROUP to which they are assigned.

When access to at least one environment is disallowed for a user, the session option “**Environment Protection**” in the user's security profile is automatically to “Y”.

Two functions are available to disallow/allow users' access to environments:

- To disallow/allow access of various users to one environment, you use the function “**Protect environment**” (which is invoked from the Environment Maintenance selection list).
- To disallow/allow access of one user to various environments, you use the function “**Protect environments**” (which is invoked from the User Maintenance selection list).

Both functions are described below.

Protecting a Single Environment for Multiple Users

On the Environment Maintenance selection list, you mark the environment you wish to protect with “EP”.

A window will be displayed. Here you enter a “U” in the field “Protect for users/libraries”. You can also enter a Start Value (as described in the section [Finding Your Way in Natural Security](#)) for the list of users to be displayed. In addition, you can select the option “Select only disallowed ones” - in which case the list of users to be displayed will only include those users for whom access to the environment is currently disallowed.

Then, the Disallow/Allow Users screen will be displayed, showing the list of users. By default, the list contains only users of type GROUP. To switch between a list of GROUPs and a list of all three user types, you press PF5. The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

On the list, you mark the users for whom you wish to disallow/allow access to the environment.

In the “Co” column, you may mark each user with one of the following function codes:

Code	Function
ED	Disallow - The user cannot access the environment.
EA	Allow - The user may access the environment.

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each user.

Protecting Multiple Environments for a Single User

On the User Maintenance selection list, you mark the user for whom you wish to protect environments with function code “EP”.

A window will be displayed. Here you can enter a Start Value (as described in the section [Finding Your Way in Natural Security](#)) for the list of environments to be displayed; as start value, you use the database ID / file number of the environments' FNAT system file. You can also select the option “Select only disallowed environments” - in which case the list of environments to be displayed will only include those environments to which access is currently disallowed for the user.

Then, the Disallow/Allow Environments screen will be displayed, showing the list of environments. For each environment, either its system-file combination (database IDs and file numbers of system files FUSER, FDIC, FSEC and FNAT) or its ID is displayed; with PF4 you can switch between the two displays. In addition, each environment profile's alias (AL) and protection status (P) are displayed. The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

On the list, you mark the environments the access to which you wish to disallow/allow for the user.

In the “Co” column, you may mark each environment with one of the following function codes:

Code	Function
ED	Disallow - The user cannot access the environment.
EA	Allow - The user may access the environment.

You can mark one or more environments on the screen with a function code. For each environment marked, the selected functions will then be executed one after another. When processing is completed, a message will indicate the access situation now in effect for each environment.

11

Protecting DDMs On Mainframes

■ Before You Begin	178
■ Components of a File Profile	179
■ Creating and Maintaining File Profiles	183

As explained in the section [Natural Security On Different Platforms](#), the protection of DDMs with Natural Security is different on mainframe computers from that on other platforms. This section describes how to control the use of DDMs (files) on *mainframe computers*. The control of DDMs on other platforms is described in the section [Protecting DDMs On UNIX, OpenVMS And Windows](#).

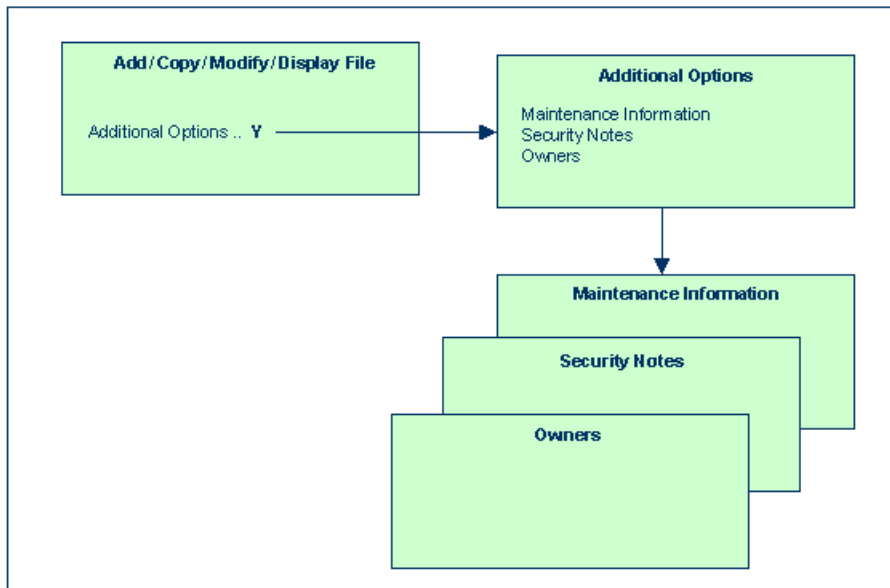
This section covers the following topics:

In Natural Security on mainframe computers, DDMs are called “files”. To define DDMs to Natural Security, you use the File Maintenance functions of Natural Security.

Before You Begin

A DDM must have been generated (in Predict, or with the Natural utility SYSDDM), before it can be defined as a file to Natural Security.

Components of a File Profile



The following type of screen is the “basic” file security profile screen, which appears when you invoke one of the functions Add, Copy, Modify, Display for a file security profile:

```

10:25:36                *** Natural Security ***                2009-07-31
                        - Modify File -

File ID .. EMPLOYEES                Modified .. 2009-07-13 by SAG
DBID .....    10
FNR .....    16
Status ... PUBL (PUBL, ACCE, PRIV)

-- DDM Modifiers --
_____  -
_____  -
_____  -
_____  -
_____  -
_____  -
_____  -
_____  -

Additional Options ... N
  
```

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

The individual items you may define as part of a file security profile are explained below.

Field	Explanation						
File ID (display only)	<p>The ID by which the file is defined to Natural Security and for which a DDM exists in the Natural system file.</p> <p>The file ID by which a file is defined to Natural Security must be identical to that of the DDM. A file ID may be up to 32 characters long and must be unique among all file IDs defined to Natural Security.</p>						
DBID / FNR (display only)	The database ID and file number of the database file referenced by the DDM. These values are taken from the DDM and written into the security profile.						
Status	<p>You may set the file status to one of the following:</p> <table> <tr> <td>PUBL</td><td>Public (not protected)</td></tr> <tr> <td>ACCE</td><td>Access (update-protected)</td></tr> <tr> <td>PRIV</td><td>Private (read- and update-protected)</td></tr> </table> <p>When you create a file security profile, the file status will, by default, be set to "PUBL". See File Status below for details.</p>	PUBL	Public (not protected)	ACCE	Access (update-protected)	PRIV	Private (read- and update-protected)
PUBL	Public (not protected)						
ACCE	Access (update-protected)						
PRIV	Private (read- and update-protected)						
DDM Modifiers	<p>You may enter up to eight IDs of users; only these users will then be allowed to maintain the DDM in Predict (or with Natural's SYSDDM utility). If you do not specify any DDM modifier, the owners of the security profile (see Additional Options below) may maintain the DDM. If neither DDM modifiers nor owners are specified, maintenance of the DDM is not restricted.</p> <p>Next to the ID of each DDM modifier, you may optionally specify a number from 1 to 3; this number determines how many of the other DDM modifiers specified must countersign for maintenance permission (the countersignature logic which applies to DDM maintenance permission is analogous to that of owners and co-owners as described in the section Countersignatures).</p>						

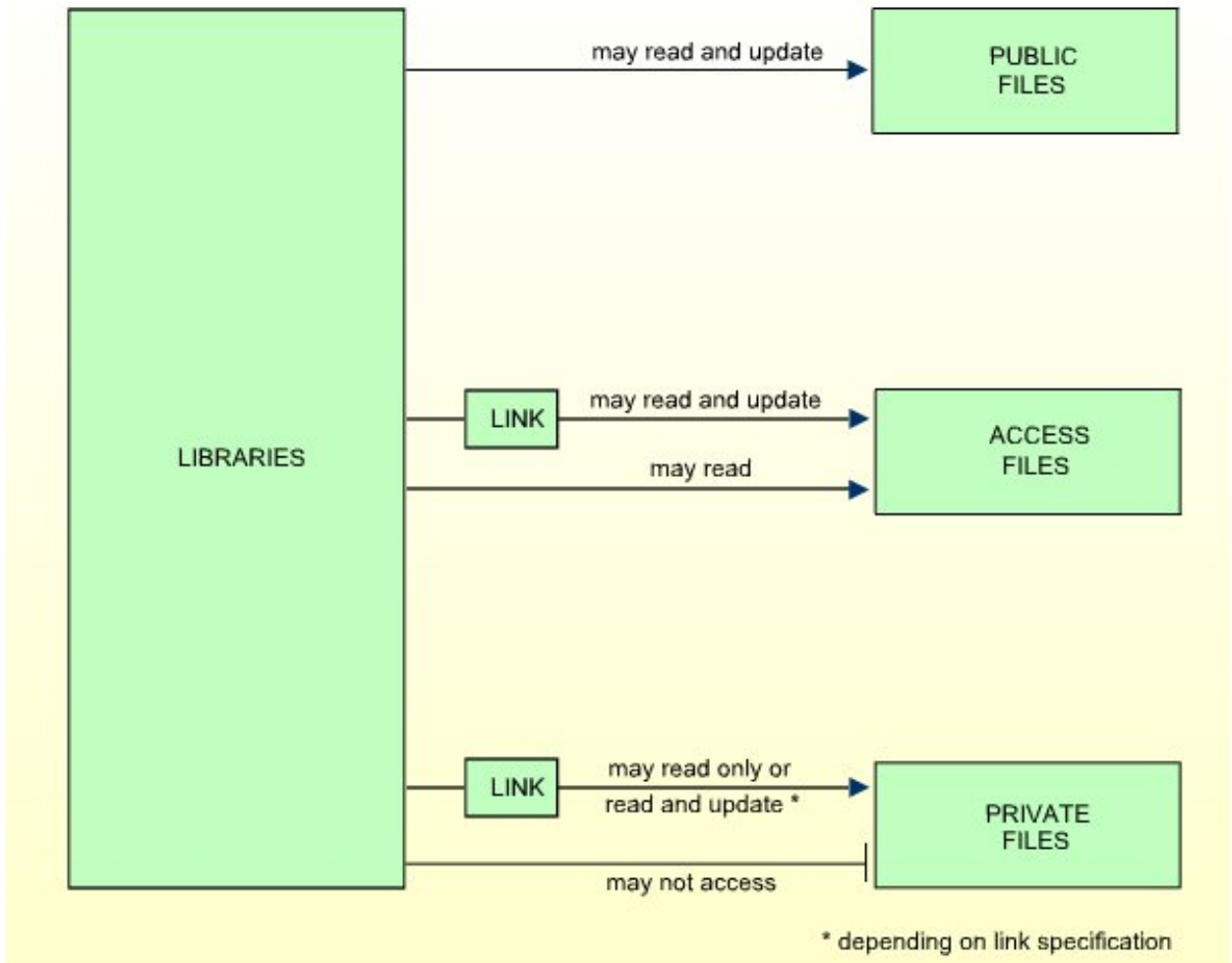
File Status

The file status of a file may be one of the following:

PUBL	PUBLIC: The file is <i>not</i> protected. It may be read and updated by any library.
ACCE	ACCESS: The file is protected as far as update is concerned. It may be read by any library. However, it may be updated only by libraries that have been linked to the file.
PRIV	PRIVATE: The file is protected. It may be accessed only by libraries that are linked to it. A link to a PRIVATE file may be specified as "read"(that is, read only) or "update" (which implies read).

The check whether a program may use a file is done when the program is *compiled*.

The following diagram illustrates the possible relationships between libraries and files in dependence of the file type:



To allow a library access to a file with status **PRIVATE** or **ACCESS**, a *link* has to be established between the library and the file. For information on how to link libraries to files, see [Linking Libraries to Files](#) below.

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none">■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation;■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	<p>In this window, you may enter your notes on the security profile.</p>
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this file security profile or link libraries to it. If no owner is specified, any user of type ADMINISTRATOR may maintain and link the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance/link permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures .</p>

Creating and Maintaining File Profiles

This section describes the functions used to create and maintain file profiles. It covers the following topics:

- [Invoking File Maintenance](#)
- [Selecting a File or DDM for Processing](#)
- [Add File](#)
- [Copy File](#)
- [Modify File](#)
- [Delete File](#)
- [Display File](#)
- [Linking Libraries To Files](#)

Invoking File Maintenance

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark the object type "File" with a character or with the cursor. The File Maintenance selection list will be displayed.

From this selection list, you invoke all file maintenance functions as described below.

Selecting a File or DDM for Processing

When you invoke File Maintenance, a list of all files that have been defined to Natural Security will be displayed.

If you do not wish to get a list of all existing files but would like only certain files to be listed, you may use the Start Value and Type/Status options as described in the section [Finding Your Way In Natural Security](#).

On the Main Menu, enter the code "M" for "Maintenance". A window will be displayed. In the window, mark the object type "File" with a character or with the cursor (and, if desired, type in a start value and/or file status). The File Maintenance selection list will be displayed:

12:50:20	*** Natural Security ***	2009-07-31
	- File Maintenance -	
Co	File ID	Status Message
—	ANGLOFILE	PUBL
—	AUTOMOBILES	PUBL
—	CLIENTES	PUBL

```
___ DELINCUENTES          PUBL
___ EMPLEADOS             PUBL
___ FAHRZEUGE             PRIV
___ FINANCE               PUBL
___ IMPUESTOS             PUBL
___ INVOICE               PUBL
___ MITARBEITER           PUBL
___ NAILFILE              PUBL
___ NEWFILE               PUBL
___ OLDFILE               PUBL
___ OTRASCOSAS            PUBL
___ PRO-FILE              PUBL

Command ==>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help      Exit      Flip  -      +      Canc
```

For each file, the file ID and file status are displayed.

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

Status as Selection Criterion

If you wish to list only DDMs of a specific status, you can specify one of the following selection criteria in the Status field above the list:

PUBL	All DDMs of status PUBLIC.
ACCE	All DDMs of status ACCESS.
PRIV	All DDMs of status PRIVATE.
DEFI	Defined; that is, all DDMs of status PRIV, ACCE, and PUBL (*).
UNDF	Undefined; that is, all DDMs whose status is not PRIV, ACCE or PUBL (*).
DDM	All defined and undefined DDMs (*).
NDDM	DDM security profiles for which no corresponding DDMs exist (*).

* This is not an actual DDM status, but for selection purposes only.

The default status for selection is “DDM”; that is, *all* DDMs will be listed.

Selecting a Function

The following file maintenance functions are available (possible code abbreviations are underlined):

Code	Function
<u>A</u> D	Add file
<u>C</u> O	Copy file
<u>M</u> O	Modify file
D <u>E</u>	Delete file
<u>D</u> I	Display file
L <u>L</u>	Link libraries to file

To invoke a specific function for a file, mark the file with the appropriate function code in column "Co".

You may select various files for various functions at the same time; that is, you can mark several files on the screen with a function code. For each file marked, the appropriate processing screen will be displayed. You may then perform for one file after another the selected functions.

Add File

This function is used to define DDMS to Natural Security, that is, create new file security profiles.

On the Main Menu, enter "M" for "Maintenance". A window will be displayed. In the window, mark object type "File" with a character and enter "UNDF" in the "Type/Status" field (and, if desired, enter a start value).

The File Maintenance selection list will be displayed, listing all files with file status "UNDEFINED" (that is, all DDMS that have been generated but not yet been defined to Natural Security).

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

On the File Maintenance selection list, mark the DDM for which you wish to create a file security profile with function code "AD". The Add File screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of a file security profile are described under *Components of a File Profile* above.

When you add a file, the owners specified in your own user security profile will automatically be copied into the file security profile you are creating.

Copy File

This function is used to define a new file to Natural Security by creating a security profile which is identical to an already existing file security profile.

What is Copied?

All components of the existing security profile will be copied into the new file security profile - except the file number and database ID (these are taken from the DDM), and the owners (these will be copied from your own user security profile into the new file security profile you are creating).

Any links existing to the existing file will *not* be copied.

How to Copy

On the File Maintenance selection list, mark the file whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, enter the ID of the new file.

The new security profile will be displayed.

The individual components of the security profile you may define or modify are described under [Components of a File Profile](#) above.

Modify File

This function is used to change an existing file security profile.

On the File Maintenance selection list, mark the file whose security profile you wish to change with function code "MO". The security profile of the selected file will be displayed.

The individual components of the security profile you may define or modify are described under [Components of a File Profile](#) above.

Delete File

This function is used to delete an existing file security profile.

On the File Maintenance selection list, mark the file you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete File function and should then decide against deleting the given file security profile, leave the Delete File window by pressing ENTER without having typed in anything.
- If you wish to delete the given file security profile, enter the file's ID in the window to confirm the deletion.

When you delete a file, all existing links to the file will also be deleted.

When you delete a file security profile, the DDM itself will not be deleted. The file ID will remain in the File Maintenance selection list with File Status set to “UNDEFINED”.

If a DDM is uncataloged in SYSDDM, deleted with SYSMAIN, or scratched in SYSDIC (Predict), the corresponding Natural Security file profile will automatically be deleted.

If you mark more than one file with “DE”, a window will appear in which you are asked whether you wish to confirm the deletion of each file security profile by entering the file's ID, or whether all files selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a file accidentally.

Display File

This function is used to display an existing file security profile.

On the File Maintenance selection list, mark the file whose security profile you wish to view with function code “DI”. The security profile of the selected file will be displayed.

The individual components of the security profile are described under [Components of a File Profile](#) above.

Linking Libraries To Files

To allow a library access to a file, a *link* has to be established between the library and the file.

Two functions are available to establish and maintain these links:

- To link *one library* to *various files*, you use the function “Link library to files” (which is invoked from the Library Maintenance selection list).
- To link *multiple libraries* to *one file*, you use the function “Link libraries to file” (which is invoked from the File Maintenance selection list).

Both functions are described below. Possible link types are summarized at the end of this section.

Linking a Single Library to Files

When you invoke the function “Link Library to Files” from the Library Maintenance selection list, a list of all files with file status ACCESS and PRIVATE will be displayed. On the list you may mark the files to which you wish to link the given library.

On the Library Maintenance selection, mark the library you wish to link with function code “LF”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a start value (as described in the section *Finding Your Way in Natural Security*) for the list of files to be displayed.
- **Selection criterion** - N = none: all files will be listed; L = linked: only files to which the library is already linked will be listed; U = unlinked: only files to which the library is not yet linked will be listed.

Then, the Link Library To Files selection list will be displayed, showing the list of files.

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

In the “Co” column you may mark each file with one of the following function codes (possible code abbreviations are underlined):

Code	Function
RE	Read-Link - The library thus linked may only read the file, but not update it.
UP	Update-Link - The library thus linked may read and update the file.
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display File - The file security profile will be displayed.

You can mark one or more files on the screen with a function code. For each file marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between the library and each file.

Linking Multiple Libraries to a File

When you invoke the function “Link Libraries to File” from the Library Maintenance selection list, a list of all libraries that have been defined to Natural Security will be displayed. On the list you may mark the libraries you wish to be linked to the given file.

On the File Maintenance selection list, mark the file to which you wish to link libraries with function code “LL”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a start value (as described in the section *Finding Your Way in Natural Security*) for the list of libraries to be displayed.
- **Libraries/Private libraries** - This options allows you to list only private libraries: if you specify "L", the list will include either all libraries including private ones (if private libraries are used in public mode) or all libraries except private ones (if private libraries are used in private mode); if you specify "U", the list will include only users' private libraries.
- **Selection criterion** - N = none: all libraries will be listed; L = linked: only libraries which are already linked to the file will be listed; U = unlinked: only libraries which are not yet linked to the file will be listed.

Then, the Link Libraries To File selection list will be displayed, showing the list of libraries.

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

In the “Co” column you may mark each library with one of the following function codes (possible code abbreviations are underlined):

Code	Function
RE	Read-Link - The library thus linked may only read the file, but not update it.
UP	Update-Link - The library thus linked may read and update the file.
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display Library - The library security profile will be displayed.

You can mark one or more libraries on the screen with a function code. For each library marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between the file and each library.

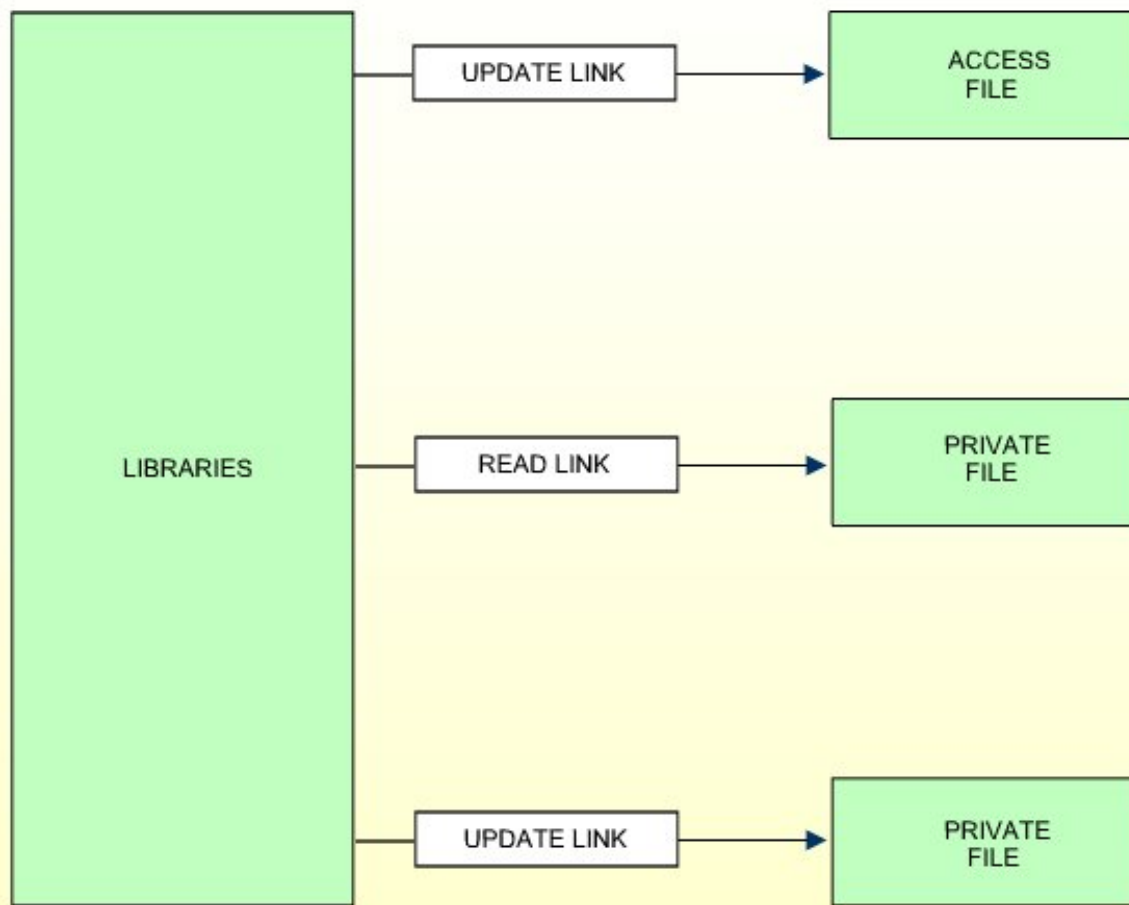
Possible Link Types

A link can only be established to a PRIVATE or ACCESS file, since there is no link required to read or update a PUBLIC file.

A link to a PRIVATE file can be specified as read-link (RE) or update-link (UP).

A link to an ACCESS file can only be specified as update-link (UP), since no link is required to read an ACCESS file.

The following figure shows all possible link types:



12

Protecting DDMs On UNIX, OpenVMS And Windows

■ Status of a DDM	192
■ DDM Security Profiles	196
■ Creating and Maintaining DDM Security Profiles	199
■ Add DDM Profile	200
■ Copy DDM Profile	201
■ Modify DDM Profile	201
■ Delete DDM Profile	201
■ Display DDM Profile	202
■ Copy Link to All Special Links	202
■ Linking a Library to a Protected DDM	203

As explained in the section [Natural Security On Different Platforms](#), the protection of DDMs with Natural Security is different on mainframe computers from that on other platforms. This section describes how to control the use of DDMs under *UNIX*, *OpenVMS* and *Windows*. The control of DDMs on mainframe computers is described in the section [Protecting DDMs On Mainframes](#).

This section covers the following topics:

FDDM Profile Parameter

With the Natural profile parameter FDDM, you can specify a system file as central location on which DDMs are to be stored (outside of libraries). If the FDDM parameter is set, DDM security profiles can only be created and maintained for DDMs contained in the library SYSTEM on that system file. Existing security profiles/settings/links for DDMs contained in other libraries are not lost, but they will not be visible within Natural Security and will have no effect.

If a central system file for DDMs is specified with the FDDM parameter, the protection of UNIX, OpenVMS and Windows DDMs and the maintenance of their security profiles is performed in the same way as with the File Maintenance functions for mainframe DDMs described in the section [Protecting DDMs On Mainframes](#).

Status of a DDM

Before a DDM can be used under Natural Security, its *status* must be defined in Natural Security. This status determines if the DDM can be used, that is, referenced in a database access statement (for example, READ, FIND, HISTOGRAM, STORE, UPDATE, DELETE) within a program.



Note: Program in this context means any type of Natural programming object that can contain database access statements; that is, programs, subprograms, subroutines etc.

A DDM whose status is not defined, cannot be referenced.

For every DDM that is to be used, two status classifications have to be made in Natural Security:

- an *internal status* and
- an *external status*.

Internal Status

The internal status controls the use of the DDM *within* the library in which it is contained.

The internal status of a DDM may be one of the following:

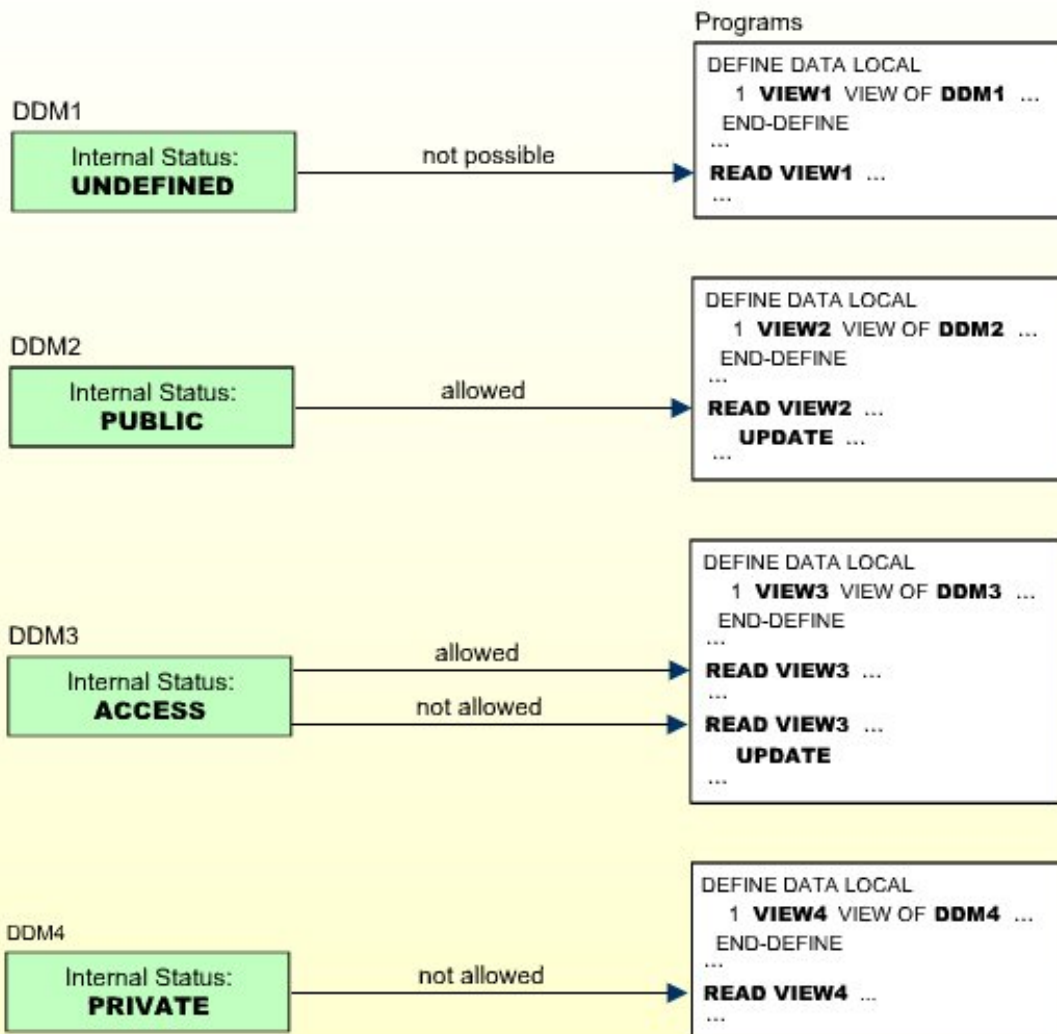
PUBLIC	The DDM can be read and updated by all programs within the library.
ACCESS	The DDM can be read, but not updated, by all programs within the library.
PRIVATE	The DDM cannot be used by any program within the library.

The internal status only applies within the library in which the DDM is contained.

The check whether a program may use a DDM is made when the program is *compiled*.

The following diagram shows how the internal status affects the use of a DDM within a library:

Library XYZ



External Status

The external status controls the use of the DDM *by other libraries*.

This requires that the library containing the DDM is used as a steplib by these other libraries. Libraries for which the library containing the DDM is not a steplib, cannot use the DDM anyhow.

The external status of a DDM may be one of the following:

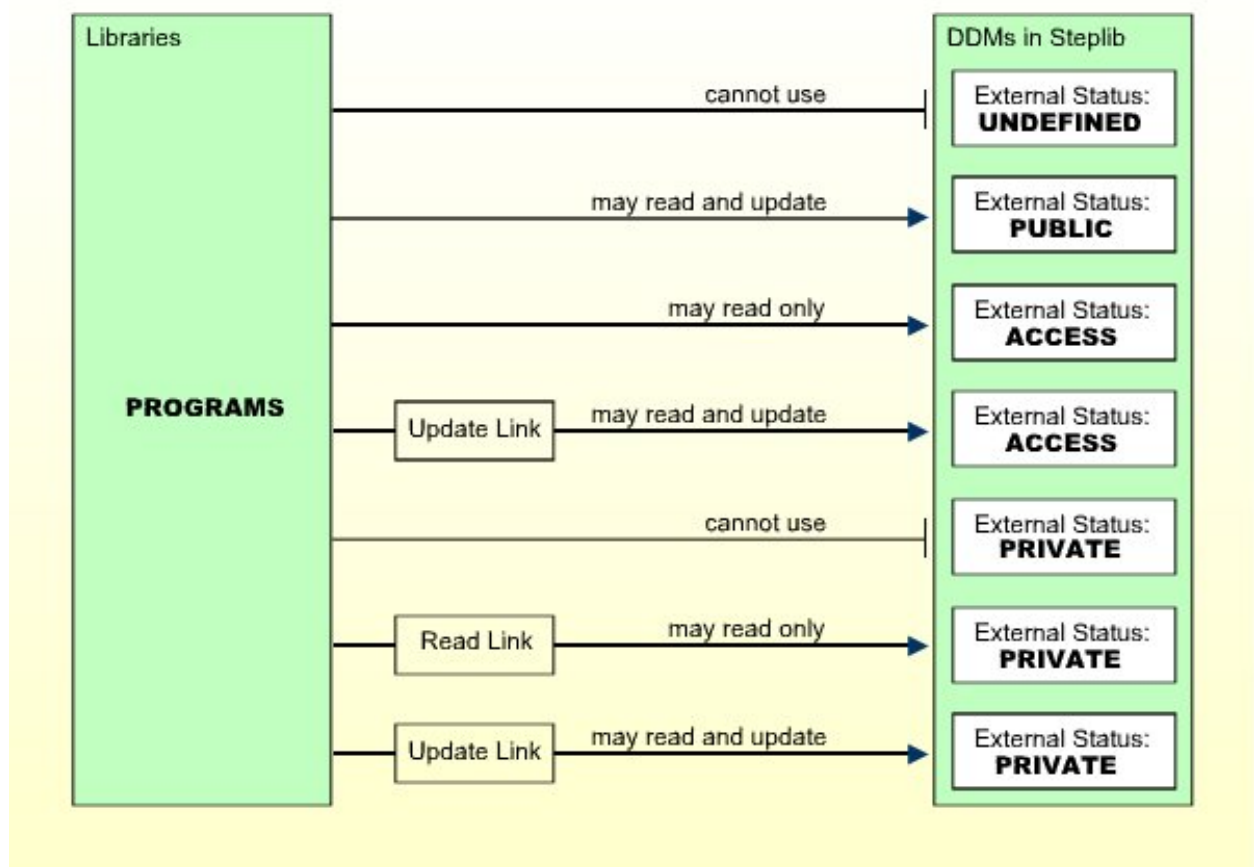
PUBLIC	The DDM is <i>not</i> protected. It can be used - that is, read and updated - by any library.
ACCESS	The DDM is protected as far as update is concerned. It can be read by any library. It may, however, be updated only by libraries which have been <i>linked</i> to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been <i>linked</i> to it. This <i>link</i> may be defined as “read” (that is, read only) or “update” (which implies read).

The external status of a DDM is only relevant if the library that contains the DDM is used as steplib by other libraries.

To allow a library to use a protected DDM in one of the library's steplibs, you have to define a *link* between the library and the DDM.

A link to a DDM whose external status is PRIVATE can be defined as “read link” or “update link”. A link to a DDM whose external status is ACCESS can only be an “update link”.

The possible relationships between libraries and DDMs in a steplib are shown in the following diagram:





Note: A link can only be established to a DDM whose external status is ACCESS or PRIVATE, because no link is required to read or update a DDM whose external status is PUBLIC.

The check whether a program may use a DDM in a steplib is made when the program is *compiled*.

For information on how to link a library to a DDM, see [Linking a Library to a Protected DDM](#) below.

The Initial Status of a DDM

The initial internal and external status of a newly generated DDM depends on the option “[Set Status of DDMs](#)”, which is set in the Restrictions window of the library profile (see Components of a Library Profile in the section *Library Maintenance*).

This option affects all DDMs in the library for which no security profiles have been defined.

By default, this option is set to “UNDF”; that is, both the internal and the external status of a new DDM are undefined to start with. Before a new DDM can be used by any program, you have to create a security profile for it and define its internal and external status in the profile.

If you set the option to “PUBL”, both the internal and external status of all newly generated DDMs are automatically set to PUBLIC. This means that new DDMs can be used by any program within the same library and in libraries that use the library as steplib. If you do not wish to restrict the use of these DDMs, you need not create security profiles for them or make any further security specifications. If you wish to restrict the use of one of these DDMs, you have to define a security profile for it, and in the profile, change the internal and external status as desired.

If you reset the option “Set status of DDMs” from “PUBL” to “UNDF”, the internal and external status of all PUBLIC DDMs without security profiles will be reset to being undefined.

DDM Security Profiles

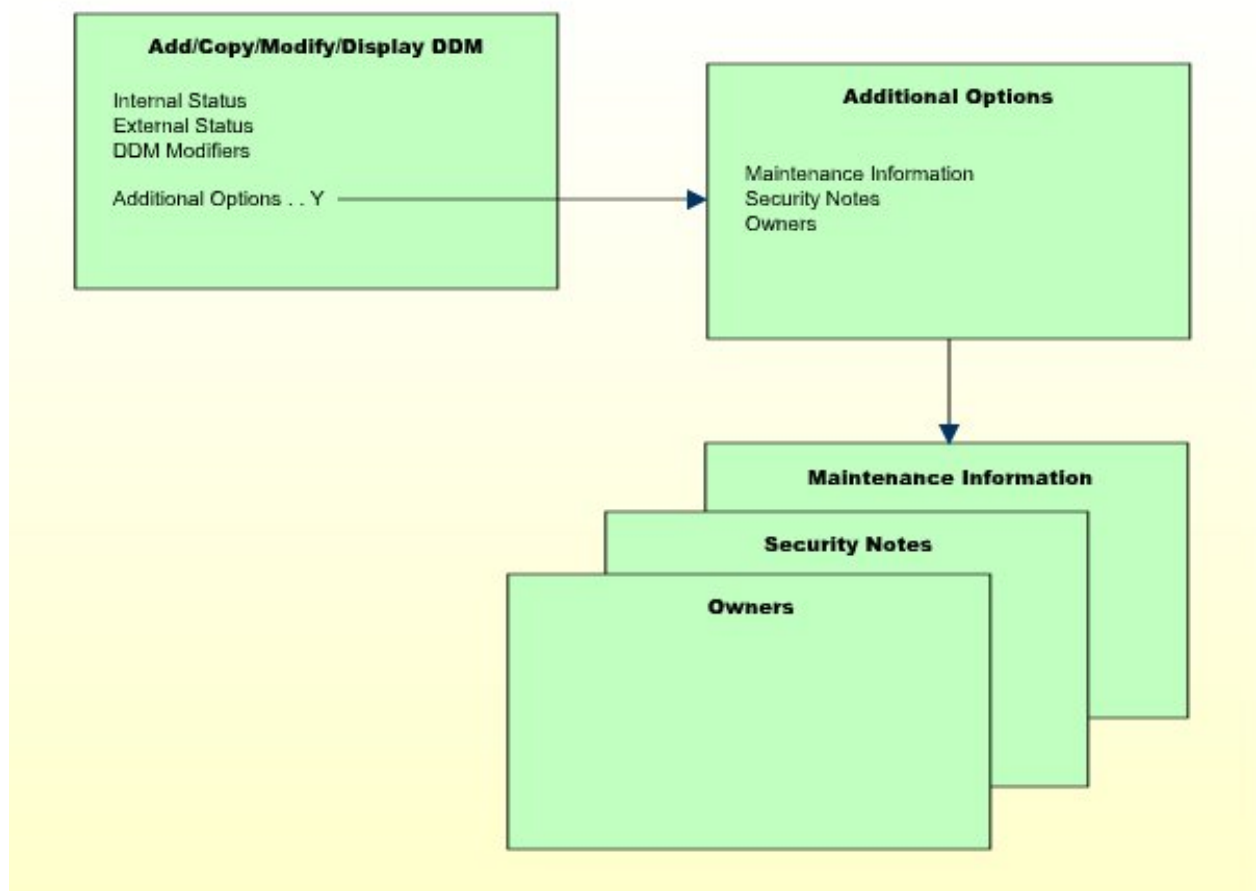
Unless the *initial status* of a DDM is automatically set to PUBLIC (see above), you have to define a security profile for every DDM that is to be used.

Apart from the internal and external status of a DDM, you can also specify some other options in a DDM security profile:

- You can restrict maintenance of the DDM itself to specific users (DDM modifiers).
- You can restrict maintenance of the DDM security profile to specific users (owners).
- You can enter notes on the security profile.

These options are explained below.

Components of a DDM Security Profile



Field	Explanation
DDM Name (display only)	The name under which the DDM was generated.
DBID / FNR (display only)	The database ID and file number of the database file referenced by the DDM.
Internal Status / External Status	See Status of a DDM above for an explanation. Possible values are:
	PUBL PUBLIC
	ACCE ACCESS
	PRIV PRIVATE
	When you create a DDM security profile, the internal and external status will, by default, be set to "PUBL".

Field	Explanation
DDM Modifiers	<p>You may enter up to eight IDs of users; only these users will then be allowed to maintain the DDM in Predict (or with Natural's DDM Services).</p> <p>If you do not specify any DDM modifier, the owners of the security profile (see Additional Options below) may maintain the DDM.</p> <p>If neither DDM modifiers nor owners are specified, maintenance of the DDM is not restricted.</p> <p>Next to the ID of each DDM modifier, you may optionally specify a number from 1 to 3; this number determines how many of the other DDM modifiers specified must countersign for maintenance permission (the countersignature logic which applies to DDM maintenance permission is analogous to that of owners and co-owners; see the section Countersignatures).</p>

Additional Options

If you mark the field “Additional Options” on the basic security profile screen with “Y”, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+). You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this DDM security profile or link libraries to it.</p> <p>If no owner is specified, any user of type ADMINISTRATOR may maintain and link the security profile.</p>

Additional Option	Explanation
	For each owner, the number of co-owners whose countersignatures will be required for maintenance/link permission may optionally be specified in the field after the ID.
	For an explanation of owner and co-owners, see the section Countersignatures .

Creating and Maintaining DDM Security Profiles



Note: If the Natural profile parameter FDDM is set, DDM security profiles can only be created and maintained for DDMs contained in the library SYSTEM.

On the Library Maintenance selection list, you mark a library with the code “MD” (or, in the case of a private library - if private libraries are used in private mode - you mark the user with the same ID on the User Maintenance selection list with the code “MD”).

A window will be displayed, in which you can enter a start value for the list of DDMs (as described in the section [Finding Your Way In Natural Security](#)).

Then a list of the DDMs contained in the library will be displayed.

For each DDM, the DDM name, the library ID, and the internal and external status are displayed. If a security profile exists for a DDM, this will be indicated in Column P.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

External Status as Selection Criterion

If you wish to list only DDMs of a specific status, you can specify one of the following selection criteria in the External Status field above the list:

PUBL	All DDMs of status PUBLIC.
ACCE	All DDMs of status ACCESS.
PRIV	All DDMs of status PRIVATE.
DEFI	Defined; that is, all DDMs of status PRIV, ACCE, and PUBL (*).
UNDF	Undefined; that is, all DDMs whose status is not PRIV, ACCE or PUBL (*).
DDM	All defined and undefined DDMs (*).
NDDM	DDM security profiles for which no corresponding DDMs exist (*).

* This is not an actual DDM status, but for selection purposes only.

The default status for selection is “DDM”; that is, *all* DDMs will be listed.

Selecting a Function

From the DDM list, you invoke all functions for creating and maintaining DDM security profiles. The following functions are available (possible code abbreviations are underlined):

Code	Function
<u>A</u> D	Add DDM Profile
<u>C</u> O	Copy DDM Profile
<u>M</u> O	Modify DDM Profile
D <u>E</u>	Delete DDM Profile
<u>D</u> I	Display DDM Profile
C <u>U</u>	Copy Link to All Special Links

To invoke a specific function for a DDM, mark the DDM with the appropriate function code in column “Co”.

You may select various DDMs for various functions at the same time; that is, you can mark several DDMs on the screen with a function code. For each DDM marked, the appropriate processing screen will be displayed, and you can perform for one DDM after another the selected functions.

Add DDM Profile

With this function, you define a DDM to Natural Security, that is, create a new DDM security profile.

On the DDM selection list, enter “UNDF” in the field “Ext. Status”.

Only those DDMs in the library which have not yet been defined to Natural Security will be listed. (The list can be scrolled as described in the section *[Finding Your Way In Natural Security](#)*).

On the list, mark the DDM for which you wish to create a security profile with function code “AD”. The Add DDM screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of a DDM security profile are described under *[Components of a DDM Security Profile](#)* above.

When you add a DDM, the owners specified in the security profile of the library in which the DDM is contained will automatically be copied into the DDM security profile you are creating.

Copy DDM Profile

With this function, you can define a DDM to Natural Security by creating a security profile which is identical to an already existing DDM security profile in the same library.

What is Copied?

All components of the existing DDM security profile will be copied into the new DDM security profile - except the file number and database ID, and the owners (the owners will be copied from your own user security profile into the new DDM security profile you are creating).

Any links existing to the “old” DDM will *not* be copied.

How to Copy

On the DDM selection list, mark the DDM whose security profile you wish to duplicate with function code “CO”.

A window will be displayed. In this window, enter the name of the “new” DDM.

The new DDM security profile will be displayed. The individual items you may define or modify in the profile are described under [Components of a DDM Security Profile](#) above.

Modify DDM Profile

With this function, you can change an existing DDM security profile.

On the DDM selection list, mark the DDM whose security profile you wish to change with function code “MO”. The DDM security profile will then be displayed. The individual items you may define or modify are described under [Components of a DDM Security Profile](#) above.

Delete DDM Profile

With this function, you can delete an existing DDM security profile.

On the DDM Maintenance selection list, mark the DDM you wish to delete with function code “DE”. A window will be displayed.

- If you have invoked the Delete DDM function and should then decide against deleting the given DDM security profile, leave the window by pressing ENTER without having typed in anything.

- If you wish to delete the given DDM security profile, enter the DDM name in the window to confirm the deletion.

When you delete a DDM security profile, all existing links to it will also be deleted.

When you delete a DDM security profile, the DDM itself will not be deleted. The DDM name will remain in the DDM selection list with the internal status set to either “UNDF” (undefined) or “PUBL” (public), depending on the option **“Set Status of DDMs”** in the library profile (this option is described in the section *Library Maintenance*).



Note: When a DDM itself is deleted (in Predict, or with Natural's DDM Services or SYSMAIN utility), the corresponding DDM security profile will not be deleted. To list the DDM profiles without DDMs in a library, you enter “NDDM” as selection criterion for the list of DDM profiles.

If you mark more than one DDM with “DE”, a window will appear in which you are asked whether you wish to confirm the deletion of each DDM security profile by entering the DDM name, or whether all DDM profiles selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a DDM profile accidentally.

Display DDM Profile

With this function, you can display an existing DDM security profile.

On the DDM selection list, mark the DDM whose security profile you wish to view with function code “DI”. The DDM security profile will then be displayed. The individual items that are part of the profile are described under ***Components of a DDM Security Profile*** above.

Copy Link to All Special Links

With this function, you can copy an existing link between a DDM and a people-protected library, so that the same kind of link (read-link or update-link) is simultaneously established between the DDM and all users who have a special link to that library.

On the DDM selection list, mark the DDM whose link you wish to copy with function code “CU”. A message will then be displayed stating that the link has been copied.

Linking a Library to a Protected DDM

If the Natural profile parameter FDDM is not set, you link a library to protected DDMs in a steplib as follows:

1. Invoke the DDM selection list of that library (as described under [Creating and Maintaining DDM Security Profiles](#) above).
2. In the Library field above the list, enter an asterisk (*). A window will be displayed listing all steplibs defined for the library.
3. Mark the steplib which contains the DDM(s) to which you wish to link the library. A list of all DDMs in the selected steplib with external status ACCESS and PRIVATE will be displayed. The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).
4. In the "Co" column of the list, you mark one or more DDMs with one of the following function codes listed below.

If the Natural profile parameter FDDM is set, a library can only be linked to protected DDMs contained in the steplib SYSTEM. This is done as follows:

1. Invoke the DDM selection list of that library (as described under [Creating and Maintaining DDM Security Profiles](#) above).
2. A list of all DDMs in the steplib SYSTEM with external status ACCESS and PRIVATE will be displayed. The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).
3. In the "Co" column of the list, you mark one or more DDMs with one of the following function codes:

Code	Function
RE	Read-Link - The library thus linked may only read the DDM, but not update it.
UP	Update-Link - The library thus linked may read and update the DDM.
CL	Cancel - An existing link will be cancelled.
CU	Copy - An existing link between a DDM and a people-protected library will be copied, so that the same kind of link (read-link or update-link) is simultaneously established between the DDM and all users who have a special link to that library.

A link to a PRIVATE DDM can be specified as read-link (RE) or update-link (UP). A link to an ACCESS DDMs can only be specified as update-link (UP), because no link is required to read an ACCESS DDM.

13

Protecting Utilities

■ General Utility Protection Considerations	206
■ Which Utilities Can Be Protected?	206
■ Utility Profiles	207
■ Defining Default Profiles	218
■ Defining Individual Profiles - Utility Maintenance	220
■ Components of Utility Profiles	227
■ Conversion of Utility Profiles	241

This section describes how you can control with Natural Security the use of various Natural utilities. It covers the following topics:

General Utility Protection Considerations

The utility protection provided by Natural Security, as described in this section, is function-oriented, which means that it is based on the concept that you can allow or disallow individual functions of a utility. You control the use of a utility by defining *utility profiles* for it, in which you allow/disallow its functions. The utilities that can be protected in this manner are listed below.

To invoke a Natural utility, you usually enter the utility name as a system command (for example, to invoke the SYSERR utility, you enter the system command SYSERR). If a utility is invoked in this way, one of the utility profiles defined for this utility applies and controls the use of the utility - thus providing consistent protection of the utility.

Invoking a utility does not change the library you are currently in; that is, when you exit the utility, you are still in the same library from which you invoked the utility. See also the section *Utility Activation* in the *Natural Utilities* documentation.

To control the use of a utility, you need not define a library profile for the library which contains the utility. A library profile for a utility is only relevant if the utility requires access to programs in other libraries (for example, user exits contained in steplib).

If a library profile is defined for a library containing a utility, and you log on to a utility library, the same logon rules apply as for a logon to any other library (as described in the section [Logging On](#)). From within the utility library, the utility may be invoked either by entering the utility name as system command (as from any other library) or by the startup transaction "MENU" (if defined in the utility's library profile) being executed. In the latter case, however, a LOGOFF command will be performed when you exit the utility.

The utilities SYSERR and SYSMAN (and NATLOAD, NATUNLD and SYSTRANS) process the contents of libraries; if the use of these utilities is not controlled by utility profiles, the [Utilities](#) option in the library profile of the library processed applies.

Which Utilities Can Be Protected?

The use of the following Natural utilities can be controlled with utility profiles:

- [NATLOAD](#) (*)
- [NATUNLD](#) (*)
- [SYSBPM](#)

- **SYSCP - Code Page Administration**
- **SYSDB2 - Tools for DB2**
- **SYSDDM**
- **SYSERR**
- **SYSMAIN**
- **SYSOBJH - Object Handler**
- **SYSARM**
- **SYSRPC**
- **SYSTRANS (*)**

(*) These utilities are only available with Natural versions prior to 4.2 on mainframes and 6.2 on UNIX and Windows. For compatibility reasons, existing utility profiles for these utilities can still be maintained. However, as the functionality of these utilities is now provided by the SYSOBJH utility, it is recommended that **SYSOBJH** be used - and protected accordingly. A function is provided which allows you to convert existing profiles for the old utilities into corresponding SYSOBJH utility profiles; it is described under *Conversion of Utility Profiles*.

Utility Profiles

This section covers the following topics:

- Types of Utility Profiles
- Default Utility Profile
- User-Specific Utility Profiles
- Library-Specific Utility Profiles
- User-Library-Specific Utility Profiles
- Which Utility Profile Applies?
- When Does a Utility Profile Take Effect?
- Available System Commands

- [Where to Define Profiles](#)

Types of Utility Profiles

Basically, a utility profile consists of a list of the utility's functions, each of which can be allowed or disallowed by marking it with "A" or "D" respectively.

For each utility listed under [Which Utilities Can Be Protected?](#) (see above), you can define:

- a default profile,
- user-specific profiles,
- library-specific profiles,
- user-library-specific profiles.

Each utility is treated individually; that is, any utility profiles only apply to the utility they are defined for, and not to any other utilities.



Note: If the use of a utility is protected by a utility profile, the Natural profile parameter settings MADIO=0 and MAXCL=0 apply automatically.

Default Utility Profile

The *default profile* of a utility applies for all users (except those for which user-specific profiles are defined). It determines which of the utility's functions the users may use and which not.

User-Specific Utility Profiles

If an individual user is to use (or not to use) other functions than the other users, you can define a *user-specific utility profile*.

Such a profile only applies to this user, it overrides the default profile, and determines which of the utility's functions this particular user may use and which not.

Example:

<p>Default Profile for SYSBPM Utility</p> <div> <p><u>Functions</u></p> <p>...</p> <p>D Delete Object from Buffer Pool Disallowed</p> <p>...</p> </div>
<p>User-Specific Profile of User UX for SYSBPM Utility</p> <div> <p><u>Functions</u></p> <p>...</p> <p>A Delete Object from Buffer Pool Allowed</p> <p>...</p> </div>

In this example, the SYSBPM function “Delete Object from Buffer Pool” is disallowed for all users - except for the user UX, for whom it is allowed.

This means that UX is the only user who may delete objects from the buffer pool.

User-specific utility profiles can be defined for users of types GROUP, ADMINISTRATOR and PERSON.

A user-specific utility profile can only be defined if a default profile (or a template) has been defined for that utility. (Templates are described under [Defining Default Profiles](#) below.)

Library-Specific Utility Profiles

Several utilities affect individual Natural libraries (for example, SYSERR can be used to maintain error messages that belong to a specific library). Generally, the utility's default profile applies to all affected libraries.

However, if some of the utility's functions are only to be allowed/disallowed for a particular library, you can define a *library-specific utility profile*.

Such a profile only applies to this library, it overrides the default profile as well as any user-specific profiles for that utility, and determines which of the utility's functions may be applied to this library and which not.

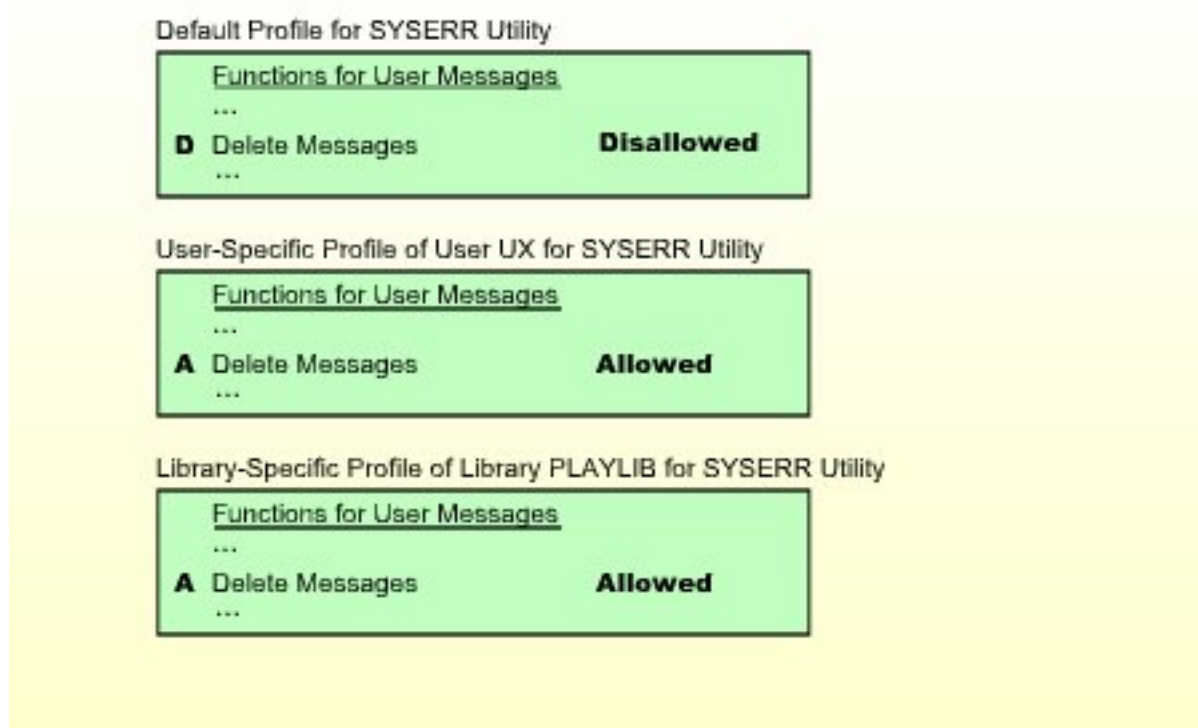
Example 1:

Default Profile for SYSERR Utility		
Functions for User Messages		
...		
A	Delete Messages	Allowed
...		
Library-Specific Profile of Library MYLIB for SYSERR Utility		
Functions for User Messages		
...		
D	Delete Messages	Disallowed
...		

In this example, the SYSERR function “Delete messages” is allowed for all libraries - except for the library MYLIB, for which it is disallowed.

This means that all users can delete user error messages from any library, except from library MYLIB. No-one can delete messages from MYLIB.

(If any user-specific profiles were defined for SYSERR, they would apply to all other libraries, but not to library MYLIB.)

Example 2:

In this example, the SYSERR function “Delete messages” is disallowed for all libraries - except for the library PLAYLIB, for which it is allowed. For the user UX, the function “Delete messages” is allowed for all libraries.

This means that all users can delete error messages from library PLAYLIB. However, no user - except user UX - can delete messages from any other library. User UX is the only user who may delete messages from any library (including PLAYLIB).

Please note that user UX's permission to delete messages from PLAYLIB depends on the library-specific profile, not the user-specific profile.

Library-specific utility profiles can be defined for the following utilities: NATLOAD, NATUNLD, SYSBPM, SYSDDM, SYSERR, SYSMAIN, SYSOBJH, SYSTRANS.

A library-specific utility profile can only be defined if a default profile has been defined for that utility.

User-Library-Specific Utility Profiles

As described above, several utilities affect individual Natural libraries. Two kinds of situations may occur in which a *user-library-specific utility profile* may have to be defined:

- A *user-specific* utility profile determines which of a utility's functions a particular user may use, regardless of the libraries which are affected by the functions (provided that no *library-specific* profiles are defined for this utility). However, if this user is to have different function usage permissions for a particular library affected by the utility's functions, you can define these in a *user-library-specific* utility profile.
- A *library-specific* utility profile determines which of a utility's functions may be used when applied to a particular library; for this library, it applies for all users (regardless of any *user-specific* profiles). However, if a particular user is to have different function usage permissions for this library, you can define these in a *user-library-specific* utility profile.

A *user-library-specific* profile only applies for one user and one library, it overrides the library-specific utility profile of that library as well as the user-specific profile of that user, and it determines which of the utility's functions the user may use for this library.

Example 1:

Default Profile for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
D	Modify Messages	Disallowed
D	Delete Messages	Disallowed

User-Specific Profile of User UX for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
A	Modify Messages	Allowed
D	Delete Messages	Disallowed

User-Library-Specific Profile of User UX for Library MYLIB for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
A	Modify Messages	Allowed
D	Delete Messages	Allowed

In this example, the SYSERR function “Delete messages” is disallowed for all users (due to the default profile). The SYSERR function “Modify messages” is also disallowed for all users (due to the default profile) - except for user UX, for whom it is allowed (due to his/her user-specific profile). Also, for the user UX both functions are allowed for the library MYLIB (due to the user-library-specific profile).

This means that no user can modify or delete any error messages from any library. The only exception is user UX: User UX may modify messages from any library; moreover, user UX may delete messages from library MYLIB (but not from any other library).

Please note that user UX's permission to modify messages from MYLIB depends on the user-library-specific profile, not the user-specific profile.

Example 2:

Default Profile for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
A Modify Messages		Allowed
D Delete Messages		Disallowed

User-Specific Profile of User UX for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
A Modify Messages		Allowed
A Delete Messages		Allowed

Library-Specific Profile of Library MYLIB for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
D Modify Messages		Disallowed
D Delete Messages		Disallowed

User-Library-Specific Profile of User UX for Library MYLIB for SYSERR Utility		
<u>Functions for User Messages</u>		
...		
A Modify Messages		Allowed
D Delete Messages		Disallowed

This example results in the following setup:

- Error messages of library MYLIB may only be modified by user UX.
- Error messages of any other library may be modified by any user.
- Error messages of library MYLIB cannot be deleted by any user.
- Error messages of any other library may only be deleted by user UX, but not by any other user.

User-library-specific utility profiles can be defined for the following utilities: NATLOAD, NATUNLD, SYSBPM, SYSDDM, SYSERR, SYSMAIN, SYSOBJH, SYSTRANS.

A user-library-specific utility profile can only be defined for a user for which a user-specific utility profile has been defined.

Which Utility Profile Applies?

When a user tries to use a utility function, Natural Security searches for the appropriate utility profile to determine whether the user is allowed to perform the function.

As shown below, you can influence the search sequence with the Session Options **Privileged Groups** and ***GROUP Only**, which can be set in a utility's default profile.

If **"*GROUP Only"** is set to **"N"**, Natural Security searches for the following utility profiles in the following order:

1. the *user-library-specific* profile
 - a. of the *user* for the library affected (only if the user is of type A or P);
 - b. of a *privileged group* for the library affected (only if **"Privileged Groups"** is set to **"Y"**);
 - c. of the *current group* in which the user is contained for the library affected;
 - d. of *another group* in which the user is contained for the library affected;
2. the *library-specific* profile of the library affected;
3. the *user-specific* profile
 - a. of the *user* (only if the user is of type A or P);
 - b. of a *privileged group* (only if **"Privileged Groups"** is set to **"Y"**);
 - c. of the *current group* in which the user is contained;
 - d. of *another group* in which the user is contained;
4. the utility's *default* profile.

If **"*GROUP Only"** is set to **"Y"**, Natural Security searches for the following utility profiles in the following order:

1. the *user-library-specific* profile
 - a. of the *user* for the library affected (only if the user is of type A or P);
 - b. of the *current group* in which the user is contained for the library affected;
2. the *library-specific* profile of the library affected;
3. the *user-specific* profile
 - a. of the *user* (only if the user is of type A or P);
 - b. of the *current group* in which the user is contained;
4. the utility's *default* profile.

For the search, the user and current group are determined by the current values of the Natural system variables ***USER** and ***GROUP** respectively. Privileged groups are the groups which are specified as **Privileged Groups** in the user's security profile; their IDs are processed in the sequence

in which they are specified in the user profile. IDs of other groups are processed in alphabetical order.

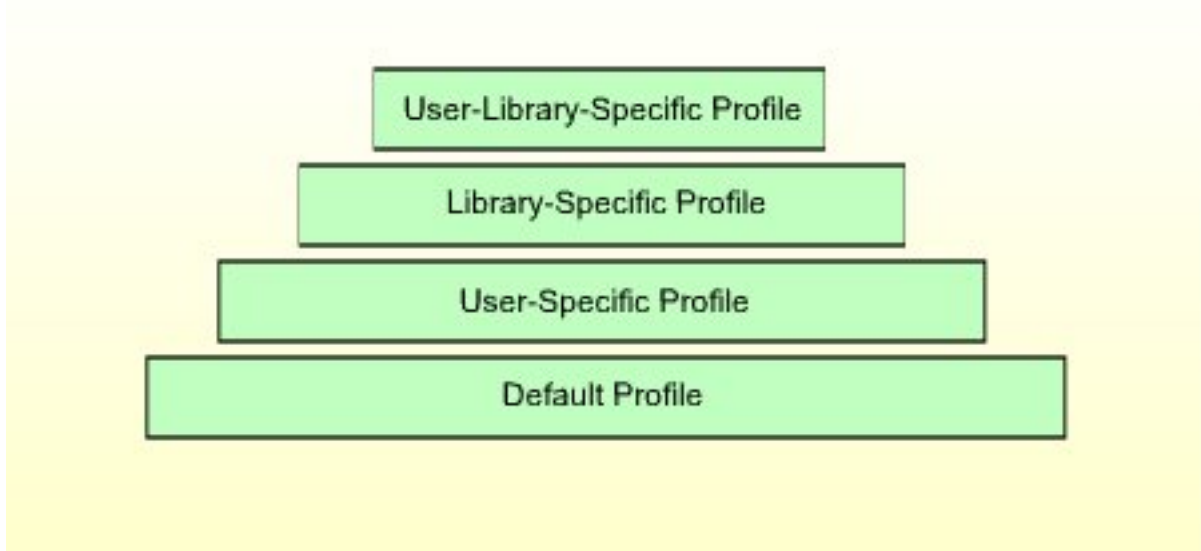
The first profile encountered in this search determines whether the user is allowed to perform the function.

If none of the above profiles exists and the utility function affects the contents of a library, the **Utilities** option in the library profile applies.

A user may obtain information about the utility profile which currently applies by using the Natural system command PROFILE (see also the **PROFILE Command** in the section *Protecting Libraries*).

The following diagram shows the hierarchy of the utility profiles.

Hierarchy of Utility Profiles



Example:

Assume the following situation: User UX (user type A), who is contained in group GX, wants to copy programming objects with the SYSMAIN utility from library LIB1 to library LIB2.

First, Natural Security checks if the user may copy programming objects with SYSMAIN *from library LIB1*; that is, if the Copy function for Programming Objects is allowed:

1. It checks the *user-library-specific* profile of user UX and library LIB1 for SYSMAIN.
2. If no such profile exists, it checks the *user-library-specific* profile of user GX and library LIB1 for SYSMAIN.
3. If no such profile exists, it checks the *library-specific* profile of library LIB1 for SYSMAIN.
4. If no such profile exists, it checks the *user-specific* profile of user UX for SYSMAIN.
5. If no such profile exists, it checks the *user-specific* profile of user GX for SYSMAIN.
6. If no such profile exists, it checks the *default* profile of SYSMAIN.

Then, Natural Security checks if the user may copy programming objects with SYSMAIN *into library LIB2*; that is, if the Copy function for Programming Objects is allowed:

1. It checks the *user-library-specific* profile of user UX and library LIB2 for SYSMAIN.
2. If no such profile exists, it checks the *user-library-specific* profile of user GX and library LIB2 for SYSMAIN.
3. If no such profile exists, it checks the *library-specific* profile of library LIB2 for SYSMAIN.

4. If no such profile exists, it checks the *user-specific* profile of user UX for SYSMAIN.
5. If no such profile exists, it checks the *user-specific* profile of user GX for SYSMAIN.
6. If no such profile exists, it checks the *default* profile of SYSMAIN.

When Does a Utility Profile Take Effect?

As the various Natural utilities and their functions differ greatly from one another, the time when Natural Security checks whether a user may use a requested utility function differs from utility to utility, and from function to function.

Available System Commands

When a user uses a utility under the control of a utility profile, the only Natural system commands available to the user within the utility are: FIN, LOGON, MAIL and PROFILE; all other system commands cannot be used. The reason for this is to preclude any “loopholes” in the protection established by the utility profiles.

Where to Define Profiles

To define *default profiles*, you use the Administrator Services section of Natural Security (as described under [Defining Default Profiles](#) below).

To define *all other utility profiles*, you use the Utility Maintenance section of Natural Security (as described under [Defining Individual Profiles - Utility Maintenance](#) below).

Defining Default Profiles

On the Main Menu, you select “Administrator Services”. The Administrator Services Menu will be displayed.



Note: [Access to Administrator Services](#) may be restricted (as explained in the section *Administrator Services*).

On the Administrator Services Menu 2, you select “Utility defaults/templates”. The Define Utility Defaults/Templates screen will be displayed, listing all the utilities for which profiles can be defined.

The status of a utility (as indicated in the Message field) can be one of the following:

Status	Meaning
Nothing defined	No profile is defined for the utility. If a utility function affects the contents of a library, its use is controlled by the Utilities option in the library security profile.
Default defined	A default profile has been defined for the utility. This default profile applies for all users for which no individual user-specific profile is defined. The Utilities option in library security profiles is ignored for this utility.
Template defined	A profile has been defined for the utility. However, this profile can only be used as a template to define individual user-specific utility profiles. If a utility function affects the contents of a library, its use is controlled by the Utilities option in the library security profile - except for those users for which a user-specific utility profile is defined.

Whether a default profile is a “real” profile or only a template is determined by the field **“Applies as Default Profile”** (see below) within the profile.



Caution: To avoid the applicability of utility profiles and the Utilities option in library profiles getting mixed up, you should always define a default profile (not only a template) for a utility if you intend to define user-specific profiles for that utility.

On the Define Utility Defaults/Templates screen, you can mark a utility with one of the following function codes:

Code	Function
AD	Define a default profile or template for the utility.
MO	Modify the utility's existing default profile or template.
DE	Delete the utility's existing default profile or template.
DI	Display the utility's existing default profile or template.

When you mark a utility with code “DE”, a window will be displayed in which you confirm the deletion by entering the utility name. When you delete a utility's default profile or template, all other profiles for that utility - that is, user-specific, library-specific and user-library-specific utility profiles - will also be deleted.

When you mark a utility with code “AD”, “MO” or “DI”, its default profile or template will be displayed.

The default profile/template for each utility provides several options, which correspond to functions of the utility concerned. The options for each utility are described under **Components of Utility Profiles** below.

You can *allow* or *disallow* each option by marking it with "A" or "D" respectively. Initially, all options are disallowed.

With PF16 and PF17, you can set all options in a utility profile simultaneously to "A" or "D" respectively.



Note: Natural Security performs consistency checks on the combinations of allowed and disallowed options - impossible combinations of "A" and "D" are automatically rejected.

Moreover, each profile provides the following field, which determines whether the profile is a “real” default profile or only a template:

Applies as Default Profile

Y	Default Profile - The profile applies for all users for which no individual utility profile is defined.
N	Template - The profile does not apply for any user. It can only be used as a template for the definition of individual user-specific utility profiles.

Once this field is set to "Y" and any user-specific or library-specific profiles have been defined for that utility, you *cannot* reset it to "N". This is to ensure consistent utility protection.

Defining Individual Profiles - Utility Maintenance

Natural Security's Utility Maintenance is used to perform all functions related to the maintenance of individual utility profiles: user-specific profiles, library-specific profiles and user-library-specific profiles.

The components of an individual profile correspond to those of the corresponding default profile; they are described under [Components of Utility Profiles](#) below.



Note: Owner logic applies to the creation/maintenance of individual utility profiles.

This section covers the following topics related to utility profile creation/maintenance:

- [Invoking Utility Maintenance](#)
- [Utility Maintenance Functions](#)
- [Adding a User-Specific Utility Profile](#)
- [Modifying/Displaying a User-Specific Utility Profile](#)
- [Deleting a User-Specific Utility Profile](#)
- [Adding a Library-Specific Utility](#)
- [Modifying/Displaying a Library-Specific Utility Profile](#)
- [Deleting a Library-Specific Utility Profile](#)
- [Adding a User-Library-Specific Utility Profile](#)
- [Modifying/Displaying a User-Library-Specific Utility Profile](#)

■ Deleting a User-Library-Specific Utility Profile

Invoking Utility Maintenance

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark object type "Utility" with a character or with the cursor. The Utility Maintenance selection list will be displayed.

The Utility Maintenance selection list shows all utilities for which either a default profile or a template has been defined. For each utility, the following information is displayed:

Default	Indicates whether a default profile has been defined for this utility (YES/NO). "NO" means that only a template has been defined.
User	Indicates whether any user-specific profiles exist for this utility (YES/NO).
Library	Indicates whether any library-specific profiles exist for this utility (YES/NO).
User-Lib.	Indicates whether any user-library-specific profiles exist for this utility (YES/NO).

Utility Maintenance Functions

From the Utility Maintenance selection list, you invoke all functions for the creation, modification, deletion and display of individual utility profiles.

The following functions are available:

Code	Function
DD	Display default profile or template. This function displays the default profile (or the template) defined for a utility.
Functions for <i>user-specific</i> utility profiles:	
DU	Display user-specific profiles. This function displays a list of existing user-specific profiles for a utility. From the list, you can select the profiles to be displayed.
AU	Add or maintain user-specific profiles. This function displays a list of users (of types A, P and G). From the list, you can select the users for which you wish to define user-specific profiles for a utility.
MU	Maintain user-specific profiles. This function displays a list of existing user-specific profiles for a utility. From the list, you can select the profiles to be maintained.
Functions for <i>library-specific</i> utility profiles:	

Code	Function
DL	Display library-specific profiles. This function displays a list of existing library-specific profiles for a utility. From the list, you can select the profiles to be displayed.
AL	Add or maintain library-specific profiles. This function displays a list of libraries. From the list, you can select the libraries for which you wish to define library-specific utility profiles.
ML	Maintain library-specific profiles. This function displays a list of existing library-specific profiles for a utility. From the list, you can select the profiles to be maintained.
Functions for <i>user-library-specific</i> utility profiles:	
DX	Display user-library-specific profiles. This function displays a list of existing user-library-specific profiles of a specific user for a utility. From the list, you can select the profiles to be displayed.
AX	Add or maintain user-library-specific profiles. This function displays a list of libraries. From the list, you can select the libraries for which you wish to define user-library-specific utility profiles for a specific user.
MX	Maintain user-library-specific profiles. This function displays a list of existing user-library-specific profiles of a specific user for a utility. From the list, you can select the profiles to be maintained.

"Add or Maintain" or "Maintain"?

The "Add or Maintain" functions (codes AU, AL, AX) display lists of all users/libraries, comprising those for which utility profiles exist as well as those for which no utility profiles have been defined. They allow you to add new utility profiles as well as modify, delete and display existing utility profiles.

The "Maintain" functions (codes MU, ML, MX) display lists of only those users/libraries for which utilities profiles exist. They allow you to modify, delete and display existing utility profiles.

You can "switch" directly from "Add or Maintain" to "Maintain" by reducing the displayed list from a list of all users/libraries to a list of only those with existing profiles. To do so, you mark with "X" the selection criterion field "U" (user-specific profile exists) "L" (library-specific profile exists) or "U-L" (user-library-specific profile exists) respectively in the heading of the list.

However, if you know beforehand that you are going to only maintain existing profiles but not add any new ones, it is recommended (for better performance) that you directly use codes MU, ML and MX respectively.

Start Values

Each of the functions listed displays a list of items (users, libraries, profiles). When you invoke a function, a window will be displayed in which you can enter a start value for the list of items to be displayed.

For functions related to *user-library-specific* profiles, the ID of the user whose user-library-specific profiles are to be listed must also be specified in the start value window.

Subfunctions

When you invoke one of the functions listed, you get a list of items (users, libraries or utility profiles).

On this list, you mark one or more items with a code to invoke a subfunction to be performed on the item.

The available subfunctions (Add, Modify, etc.) differ depending on the function invoked.

For a list of available subfunctions, you enter a question mark (?) in the field “Co”.

Information Displayed

Add/Maintain/Display User-Specific Utility Profiles

On the selection list of users displayed with function codes AU, DU and MU, the following information is displayed for each user:

Type	Indicates the user type (A, P or G).
U	An “X” indicates that the user has a user-specific profile for this utility.
U-L	An “X” indicates that the user has one or more user-library-specific profiles for this utility.

Add/Maintain/Display Library-Specific Utility Profiles

On the selection list of libraries displayed with function codes AL, DL and ML, the following information is displayed for each library:

Prot.	Indicates the “people-protected” and “terminal-protected” settings as defined in the library security profile.
Link	(empty)
L	An “X” indicates that the library has a library-specific profile for this utility.
U	An “X” indicates that the library has one or more user-library-specific profiles for this utility.

Add/Maintain/Display User-Library-Specific Utility Profiles

On the selection list of libraries displayed with function codes AX, DX and MX, the following information is displayed for each library:

Prot.	Indicates the “people-protected” and “terminal-protected” settings as defined in the library security profile.
Link	Indicates whether the user is linked to the library (LK = normal link, SL = special link).
U-L	An “X” indicates that the user has a user-library-specific profile for this library for this utility.
L	An “X” indicates that the library has a library-specific profile for this utility.

Adding a User-Specific Utility Profile

A user-specific utility profile can only be defined for a utility for which either a *default profile* or a *template* exists.

To add a user-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “AU”. A window will be displayed in which you can enter a start value for the list of users to be displayed. Then a list of users (of types A, P and G) will be displayed.

On that list, you mark the desired user with “AD”. The user-specific profile for the utility will be displayed for you to define.

The options you can allow or disallow within the profile are the same as in the corresponding default profile or template (see [Components of Utility Profiles](#) below).

The initial “allowed/disallowed” settings in the user-specific profile are taken from the default profile or the template.

Modifying/Displaying a User-Specific Utility Profile

To modify or display a user-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “MU” or “DU” respectively. A window will be displayed in which you can enter a start value for the list of user-specific profiles to be displayed. Then a list of existing user-specific profiles for the selected utility will be displayed.

On that list, you mark the desired profile with “MO” (modify) or “DU” (display) respectively. The profile will be displayed for modification/display.

The options in the profile are the same as in the corresponding default profile or template (see [Components of Utility Profiles](#) below).

Deleting a User-Specific Utility Profile

To delete a user-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “MU”. A window will be displayed in which you can enter a start value for the list of user-specific profiles to be displayed. Then a list of existing user-specific profiles for the selected utility will be displayed.

On that list, you mark the desired profile with “DE”. A window will be displayed in which you confirm the deletion.

When you delete a user-specific utility profile, all *user-library-specific* utility profiles for this user for this utility will also be deleted.

Adding a Library-Specific Utility

A library-specific utility profile can only be defined for a utility for which a *default profile* (not only a template) has been defined.

To add a library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “AL”. A window will be displayed in which you can enter a start value for the list of libraries to be displayed. Then a list of libraries will be displayed.

On that list, you mark the desired library with “AD”. The library-specific profile for the utility will be displayed for you to define.

The options you can allow or disallow within the profile are the same as in the corresponding default profile (see [Components of Utility Profiles](#) below).

The initial “allowed/disallowed” settings in the library-specific profile are taken from the default profile.

Modifying/Displaying a Library-Specific Utility Profile

To modify or display a library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “ML” or “DL” respectively. A window will be displayed in which you can enter a start value for the list of library-specific profiles to be displayed. Then a list of existing library-specific profiles for the selected utility will be displayed.

On that list, you mark the desired profile with “MO” (modify) or “DL” (display) respectively. The profile will be displayed for modification/display.

The options in the profile are the same as in the corresponding default profile (see [Components of Utility Profiles](#) below).

Deleting a Library-Specific Utility Profile

To delete a library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “ML”. A window will be displayed in which you can enter a start value for the list of library-specific profiles to be displayed. Then a list of existing library-specific profiles for the selected utility will be displayed.

On that list, you mark the desired profile with “DE”. A window will be displayed in which you confirm the deletion.

Adding a User-Library-Specific Utility Profile

A user-library-specific utility profile can only be defined for a user for which a *user-specific profile* for that utility exists.

To add a library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “AX”. A window will be displayed in which you enter the ID of the user for whom a user-library-specific profile is to be defined; also, you can enter a start value for the list of libraries to be displayed. Then a list of libraries will be displayed.

On that list, you mark the desired library with “AD”. The user-library-specific profile for the specified user for this library will be displayed for you to define.

The options you can allow or disallow within the profile are the same as in the corresponding default profile (see [Components of Utility Profiles](#) below).

The initial “allowed/disallowed” settings in the user-library-specific profile are taken from the corresponding library-specific profile; if no such profile exists, they are taken from the corresponding user-specific profile.

Modifying/Displaying a User-Library-Specific Utility Profile

To modify or display a library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “MX” or “DX” respectively. A window will be displayed in which you enter the ID of the user whose user-library-specific profile(s) are to be listed; also, you can enter a start value for the list of profiles to be displayed. Then a list of existing user-library-specific profiles of the specified user for the selected utility will be displayed.

On that list, you mark the desired profile with “MO” (modify) or “DX” (display) respectively. The profile will be displayed for modification/display.

The options in the profile are the same as in the corresponding default profile (see [Components of Utility Profiles](#) below).

Deleting a User-Library-Specific Utility Profile

To delete a user-library-specific utility profile, you mark the desired utility on the Utility Maintenance selection list with “MX”. A window will be displayed in which you enter the ID of the user whose user-library-specific profile(s) are to be listed; also, you can enter a start value for the list of profiles to be displayed. Then a list of existing user-library-specific profiles of the specified user for the selected utility will be displayed.

On that list, you mark the desired profile with “DE”. A window will be displayed in which you confirm the deletion.

Components of Utility Profiles

A utility profile provides several options which correspond to the functions of the utility concerned. These options are the same in every profile related to that utility: default profile, user-specific, library-specific and user-library-specific profiles.

The individual options are described below for each utility:

- [NATLOAD Utility Profiles](#)
- [NATUNLD Utility Profiles](#)
- [SYSBPM Utility Profiles](#)
- [SYSCP - Code Page Administration - Utility Profiles](#)
- [SYSDB2 - Tools for DB2 - Utility Profiles](#)
- [SYSDDM Utility Profiles](#)
- [SYSERR Utility Profiles](#)
- [SYSMAIN Utility Profiles](#)
- [SYSOBJH - Object Handler - Utility Profiles](#)
- [SYSPARM Utility Profiles](#)
- [SYSRPC Utility Profiles](#)
- [SYSTRANS Utility Profiles](#)
- [Additional Options](#)

NATLOAD Utility Profiles

The NATLOAD utility is only available with Natural versions prior to 4.2 on mainframes and 6.2 on UNIX and Windows. For compatibility reasons, existing utility profiles for NATLOAD can still be maintained. However, instead of NATLOAD, it is recommended that the [SYSOBJH utility](#) be used and profiles defined for it. A function is provided which allows you to convert your NATLOAD utility profiles into corresponding SYSOBJH utility profiles; it is described under [Conversion of Utility Profiles](#).

The profiles for the NATLOAD utility provide the following options:

Option	Explanation
Load Natural Objects	Determines whether the user may load programming objects.
Del.	Determines whether the user may process delete instructions for programming objects (this requires that the loading of programming objects is allowed).
Load DDMs	Determines whether the user may load DDMs.
Del.	Determines whether the user may process delete instructions for DDMs (this requires that the loading of DDMs is allowed).
Load Error Messages	Determines whether the user may load error messages.
Del.	Determines whether the user may process delete instructions for error messages (this requires that the loading of error messages is allowed).
Scan Natural Objects	Determines whether the user may scan the work file for programming objects.
Scan DDMs	Determines whether the user may scan the work file for DDMs.
Scan Error Messages	Determines whether the user may scan the work file for error messages.
PC Upload	Determine whether the user may use the NATLOAD parameters of the same names.
Replace	
New Library	

NATUNLD Utility Profiles

The NATUNLD utility is only available with Natural versions prior to 4.2 on mainframes and 6.2 on UNIX and Windows. For compatibility reasons, existing utility profiles for NATUNLD can still be maintained. However, instead of NATUNLD, it is recommended that the [SYSOBJH utility](#) be used and profiles defined for it. A function is provided which allows you to convert your NATUNLD utility profiles into corresponding SYSOBJH utility profiles; it is described under [Conversion of Utility Profiles](#).

The profiles for the NATUNLD utility provide the following options:

Option	Determines whether the user may:
Unload Natural Objects	Unload programming objects.
Unload DDMs	Unload DDMs.
Unload Error Messages	Unload error messages.
Unload Delete Instructions	Unload delete instructions.
PC Download	Use the NATUNLD parameters of the same names.
Target Library	

SYSBPM Utility Profiles

The SYSBPM utility is only available with Natural on mainframe computers.

The profiles for the SYSBPM utility provide the following options:

Object Pool Statistics

Option	Explanation
Buffer Pool	Determine whether the user may use the SYSBPM functions/commands of the same names.
- General BP Statistics	
- BP Load/Locate Statistics	
- BP Fragmentation	
- Internal Function Usage	
- BP Hash Table Statistics	
BP Cache	
- General BP Cache Statistics	
- BP Cache Call Statistics	
- BP Cache Hash Table Statistics	

Buffer Pool Library Object Maintenance

Option	Explanation
Object Functions	Determine whether the user may use the SYSBPM functions/commands of the same names.
- List Objects	
- Delete Objects	
- Directory Information	
- Hexadecimal Display	
- Write to Work File	
- Display Sorted Extract	
Functions for the Objects Displayed	
- CLEAR	
- DELETE	
- FDELETE	
- RESIDENT	
Blacklist Maintenance	
- Maintain Blacklist	
- Maintain Blacklist ADD	
- Maintan Blacklist DELETE	

Option	Explanation
- Maintain Blacklist DELETE ALL	
- Maintain Blacklist UPDATE	
- List Object Sets	
- Edit Object Set	
- Add Object Set to Blacklist	
- Delete Obj. Set from Blacklist	
Preload List Maintenance	
- List Preload Lists	
- Edit Preload List	
- Gen. Preload List from BP	

Buffer Pool Global Commands

Option	Explanation
CHECK HASH	Determine whether the user may use the SYSBPM functions/commands of the same names.
CLOSE BPC	
CLOSE HASH	
DELETE BP	
DELETE BPC	
DISPLAY CDIR	
INITIALIZE	
- INITIALIZE BP	
- INITIALIZE BPC	
REBUILD HASH	
REORG HASH	
REORGC HASH	
RESET BP	
SELECT BP	
DISPLAY BP	

SYSCP - Code Page Administration - Utility Profiles

The profiles for the SYSCP utility (Natural Code Page Administration) provide the following options:

Option	Explanation
Code Page Maintenance of Source Objects	Determine whether the user may use the Natural Code Page Administration's functions of the same names.
- List Code Page Information of Sources	
- Check Conversion of Unassigned Sources	
- Assign Code Page Information to Sources	
- Check Conversion of Assigned Sources	
- Convert to Different Code Page	
- Remove Code Page Information from Sources	
All Code Pages	
Unicode Properties	

SYSDB2 - Tools for DB2 - Utility Profiles

The SYSDB2 utility (Natural Tools for DB2) is only available with Natural on mainframe computers.

The profiles for the SYSDB2 utility provide the following options:

Option	Explanation
Application Plan Maintenance	Determine whether the user may use the Natural Tools for DB2's functions/commands of the same names.
- Prepare Job Profile	
- Create DBRM	
- Bind	
- Rebind	
- Free	
-List JCL	
- Display Job Output	
Catalog Maintenance	
Interactive SQL	
- SWL Input Member	
- Data Output Member	
Retrieval of System Tables	
- List Databases	
- List Packages	

Option	Explanation
- List Plans	
- List Tables	
- User Authorization	
- Statistic Table	
Environment Settings	
Explain PLAN_TABLE	
- List PLAN_TABLE - Latest	
- List PLAN_TABLE - All	
- Delete from PLAN_TABLE	
File Server Statistics	
DB2 Command Execution	
- Display Command	
- Display Output	

SYSDDM Utility Profiles

The SYSDDM utility is only available with Natural on mainframe computers, UNIX and OpenVMS.

The profiles for the SYSDDM utility provide the following options:

Option	Explanation
Generate DDM from Adabas FDT	Determine whether the user may use the SYSDDM functions of the same names.
Catalog DDM	
Edit DDM	
Delete DDM	
List DDMs	
List DDMs with Additional Information	
Copy DDM to Another FDIC File	
Show Defined DBIDs and Used FNRs	
SQL Services (NDB/NSQ)	
DL/I Services	
SQL Services (NSB)	
Rename DDM	

SYSERR Utility Profiles

The profiles for the SYSERR utility provide the following options:

Option	Explanation
Add New Messages	Determine whether the user may use the SYSERR functions of the same names.
Delete Messages	
Display Messages	
Modify Messages	
Print Messages	
Scan in Messages	
Select Messages from a List	
Translate Messages into Another Language	

You can allow/disallow these options separately for:

- user messages (PF7),
- Natural system messages (PF8).

In addition, by pressing PF8 again, you can allow/disallow the use of the following SYSERR direct commands:

Command	Explanation
EXPORT	Possible values for each command: <ul style="list-style-type: none"> ■ A = Command is allowed for all users. ■ R = Command is restricted: it is allowed for Natural Security administrators only. ■ D = Command is disallowed for all users.
IMPORT	
LAYOUT	
NEXT	
RESTART	
SAMPLE	
SHIFT	
TRACE	
USER	

SYSMAIN Utility Profiles

As the SYSMAIN utility is not identical on all platforms, some SYSMAIN options/functions may not be available on some platforms.

The SYSMAIN utility can be invoked in two ways:

- with the command SYSMAIN,
- via the application programming interface MAINUSER.

By default, utility profiles defined for the SYSMAIN utility apply to both ways. However, it is possible to define a separate set of utility profiles which control the use of SYSMAIN functions when invoked via MAINUSER. See [MAINUSER API](#) under Additional Options below for details.

The profiles for the SYSMAIN utility provide the following options:

Option	Explanation
Programming Objects	This general setting in the first column of the screen determines whether the user may use SYSMAIN at all for this type of object.
Debug Environments	
User Messages	If this is set to "D" (disallowed), all subordinate function specifications for this object type must also be set to "D".
DDMs	
Natural Messages	
Profiles	
Rules	
DL/I Subfiles	
Resources	

In addition, you can allow/disallow the following functions for each object type individually:

Option	Determines whether the user may use:
Co	The SYSMAIN function COPY for this type of object.
De	The SYSMAIN function DELETE for this type of object.
Fi	The SYSMAIN function FIND for this type of object.
Im	The SYSMAIN function IMPORT for this type of object.
Li	The SYSMAIN function LIST for this type of object.
Mo	The SYSMAIN function MOVE for this type of object.
Ren	The SYSMAIN function RENAME for this type of object.
Rep	The SYSMAIN function REPLACE for this type of object.
FNAT	The SYSMAIN function SET FNAT for this type of object.
FSEC	The SYSMAIN function SET FSEC for this type of object. (*)

Option	Determines whether the user may use:
FDIC	The SYSMAIN function SET FDIC for this type of object. (*)

(*) These options can be set in the default profile and in user-specific profiles, but not in library-specific or user-library-specific profiles.

SYSOBJH - Object Handler - Utility Profiles

The profiles for the SYSOBJH utility (Natural Object Handler) provide the following options:

Option	Explanation
Unload	Determine whether the user may use the Object Handler functions of the same names.
UnDeLi	
Load	
Delete	
Scan	

In addition, you can allow/disallow the above functions for each object type individually:

Option	Determines whether the function may be applied to:
Nat	Natural programming objects.
Err	Error messages.
CPr	Command processors.
NRe	Natural-related objects.
Ext	External objects.
FDT	Adabas FDTs.
MfD	Mainframe DDMs.
MfR	Mainframe-related objects.
App	Applications.
Del	This option determines whether the Object Handler parameter DELETEALLOWED may be specified for the function.
Par	This option determines whether Object Handler parameters may be specified for the function.
Rep	This option determines whether the Object Handler parameter REPLACE may be specified for the function.



Note: In library-specific and user-library-specific profiles, options applying to object types which are not library-related cannot be allowed/disallowed.

Also, the profiles for SYSOBJH provide the following general options:

Option	Explanation
Admin	Determines whether the user may use the "Admin" section of the Object Handler.
FSEC	Determines whether the user may specify the Object Handler parameters of the same names.
FDIC	
Transfer only	<ul style="list-style-type: none">■ Y = Only the transfer format may be used (processes only sources).■ N = Transfer and internal formats may be used (processes sources and cataloged objects).

In the profiles for SYSOBJH, you can also allow/disallow the following Object Handler direct commands:

Command	Explanation
Navigation Commands:	
GO	Determine whether the user may use the Object Handler direct commands of the same names.
- GO HOME	
- GO UNLOAD	
- GO LOAD	
- GO SCAN	
- GO RESTART	
- GO ADMIN	
- GO VIEW	
- GO FIND	
- GO UNDELI	
Configuration Commands:	
SET	Determine whether the user may use the Object Handler direct commands of the same names.
- SET TRACE ON	
- SET TRACE WORKFILE	
- SET TRACEFILE	
- SET FREE ON/OFF	
- SET EXECUTIONMSG ON/OFF	
- SET ADVANCEDCMD ON/OFF	
Show Commands:	
SHOW	Determine whether the user may use the Object Handler direct commands of the same names.
- SHOW LAST RESULT	
- SHOW LAST MESSAGE	
- SHOW PROFILE	

Command	Explanation
- SHOW REPORT	
- SHOW STATUS	
- SHOW TRACE	
Other Commands:	
CHANGE WORKPLAN LIBRARY	Determine whether the user may use the Object Handler direct commands of the same names.
CLEAR	
INIT	
READ PROFILE	
SETTINGS	

SYSARM Utility Profiles

The SYSARM utility is only available with Natural on mainframe computers.

The profiles for the SYSARM utility provide the following options:

Option	Explanation
List Profiles	Determine whether the user may use the SYSARM functions of the same names.
Display Profile	
Add New Profile	
Modify Profile	
Copy Profile	
Delete Profile	

SYSRPC Utility Profiles

The profiles for the SYSRPC utility provide the following options:

Option	Explanation
Parameter Maintenance	Determine whether the user may use the SYSRPC functions of the same names.
Service Directory Maintenance	
Remote Directory Maintenance	
Stub Generation	
Terminate Server	

SYSTRANS Utility Profiles

The SYSTRANS utility is only available with Natural versions prior to 4.2 on mainframes and 6.2 on UNIX and Windows. For compatibility reasons, existing utility profiles for SYSTRANS can still be maintained. However, instead of SYSTRANS, it is recommended that the [SYSOBJH utility](#) be used and profiles defined for it. A function is provided which allows you to convert your SYSTRANS utility profiles into corresponding SYSOBJH utility profiles; it is described under [Conversion of Utility Profiles](#).

The profiles for the SYSTRANS utility provide the following options:

Option	Determines whether the user may use:
Unload	The SYSTRANS Unload function.
Load	The SYSTRANS Load function.
Replace	The Replace option of the SYSTRANS Load function.
Scan	The SYSTRANS Scan function.
Restart	The SYSTRANS Restart function.

In addition, you can allow/disallow the above functions for each object type individually:

Option	Determines whether the function may be applied to:
NAT	Natural programming objects.
Map	Maps.
DDM	DDMs.
FDT	Adabas FDTs.
Err	Error messages.
CPr	Command processors.
Lib	Libraries.
All	All objects on the work file to be processed.

Also, the profiles for SYSTRANS provide the following options, which apply to the Direct Transfer functions of SYSTRANS:

Option	Determines whether the user may use:
Direct Transfer Functions	Any SYSTRANS Direct Transfer functions (using Natural RPC).
Transfer	The SYSTRANS function "Direct Transfer (using RPC)".
Restart	The SYSTRANS function "Restart Direct Transfer".
Report	The SYSTRANS function "Get Report from Direct Transfer Load".
Define	The SYSTRANS function "Define Local Transfer System".

Additional Options

The following Additional Options are part of the default security profiles of all utilities. They can only be set in the *default* profiles, but not in individual user-specific, library-specific or user-library-specific profiles. For each utility, the Additional Options settings apply to all utility profiles related to that utility.

If you press PF4 on a basic utility default profile screen, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners
- Session Options

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this utility security profile. If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures.</p>
Session Options	See below.

Session Options

If you mark “Session Options” in the Additional Options window with any character, the Session Options window will be displayed. In this window, you can set the following options:

Option	Explanation	
Access Recorded	This option determines whether users' access to the utility is to be recorded or not.	
	Y	Every time a user invokes the utility, a record will be written by Natural Security. You may review the use of the utilities by viewing these access records (see Logon Records in the section <i>Administrator Services</i> for further information).
	N	Access to the utility is not recorded.
Privileged Groups	With this option, you can influence the order in which Natural Security searches for the appropriate utility profile to apply. It determines whether or not utility profiles defined for groups which are specified as Privileged Groups in a user security profile are part of the search order. See the section Which Utility Profile Applies? above.	
	Y	User-library-specific and user-specific profiles of privileged groups are part of the search order.
	N	Privileged groups have no influence on the search order.
	If the option *GROUP Only (see below) is set to "Y", this option must be set to "N".	
*GROUP Only	With this option, you can influence the order in which Natural Security searches for the appropriate utility profile to apply:	
	Y	User-library-specific and user-specific profiles of the current group (as determined by the value of the Natural system variable *GROUP) are part of the search order, but those of any other group in which the user is contained are not.
	N	User-library-specific and user-specific profiles of <i>all</i> groups in which the user is contained are part of the search order.
	See the section Which Utility Profile Applies? above for details.	
MAINUSER API	This option is only available for the SYSMAIN utility. It controls the use of SYSMAIN functions invoked via the application programming interface (API) MAINUSER.	
	If you set this option to "Y", a separate entry named MAINUSER will be created on the Define Utility Defaults/Templates screen. With this, you can create a separate set of utility profiles to allow/disallow the use of SYSMAIN functions when invoked via the MAINUSER API. These profiles are independent of the "normal" SYSMAIN utility profiles which control the use SYSMAIN functions when invoked via the SYSMAIN command.	
	The components of the MAINUSER utility profiles are the same as those of the SYSMAIN utility profiles .	

Option	Explanation
Utilities option	This option is only available for the utilities SYSMAIN and SYSOBJH. It can be used to apply the "Utilities" option in library profiles to these utilities.
Y	The "Utilities" option in a library profile determines who may use SYSMAIN/SYSOBJH to process the contents of the library.
O	Same as "Y". In addition, if the "Utilities" option in a library profile is set to "O" and an owner requires a countersignature, the countersignature prompt will be suppressed; instead, the library will be excluded from SYSMAIN/SYSOBJH processing.
N	The "Utilities" option in library profiles has no effect for SYSOBJH; it has no effect for SYSMAIN if no utility profile is defined for SYSMAIN.

Conversion of Utility Profiles

This function is used to convert your old **NATLOAD**, **NATUNLD** and **SYSTRANS** utility profiles into corresponding SYSOBJH utility profiles.

The conversion results in the following:

- **Creation of new profiles:**

For every old NATLOAD/NATUNLD/SYSTRANS profile for which a corresponding SYSOBJH profile does not yet exist, such a SYSOBJH profile will be created automatically. The settings in the old profile will be mapped to the new profile.

- **Adjustments of existing profiles:**

For every old NATLOAD/NATUNLD/SYSTRANS profile for which a corresponding SYSOBJH profile already exists, the settings in the SYSOBJH profile may be adjusted automatically to reflect the settings in the old profile(s). To avoid undesired changes in existing profiles, the conversion function allows you to control and monitor which automatic adjustments are made.

The resulting set of SYSOBJH profiles will provide utility protection equivalent to that of the old profiles.

The conversion function provides information on exactly which profiles were created/adjusted and why; in addition, you can see the cause and result of each adjustment made (see option "Select listing type" below).

In any case, after you have performed the conversion, you can make further adjustments to your SYSOBJH profiles manually by modifying them with Natural Security's utility maintenance functions.

► **To invoke the conversion function:**

- Enter the direct command `CONVUTIL` in the command line within the library `SYSSEC`.

The Convert Utility Profiles screen will be displayed. It provides the options described below.

Conversion Options

The Convert Utility Profiles screen provides the following options to control the conversion process:

Option	Explanation
Select function	<p>Two functions are available:</p> <ul style="list-style-type: none"> ■ CHECK - performs a test run of the intended conversion and shows the SYSOBJH profile settings which would result from it. ■ CONVERT - performs the actual conversion and shows the resulting SYSOBJH profile settings.
Select conversion rule	<p>This option determines whether in already existing SYSOBJH profiles "allowed" settings are to overwrite "disallowed" settings, or vice versa:</p> <ul style="list-style-type: none"> ■ A - "Allow" forced: If a function is set to "A" in an old utility profile and the corresponding function in the corresponding existing SYSOBJH profile is set to "D", the "D" will be overwritten by the "A". This means that the function which previously was disallowed in the SYSOBJH profile will now be allowed. ■ D - "Disallow" forced: If a function is set to "D" in an old utility profile and the corresponding function in the corresponding existing SYSOBJH profile is set to "A", the "A" will be overwritten by the "D". This means that the function which previously was allowed in the SYSOBJH profile will now be disallowed.
Create default profile	<p>This option only applies if a default profile exists for an old utility, while for SYSOBJH only a template - but no default profile - exists. In this case, you can use this option to determine whether a default profile for SYSOBJH is to be created or not.</p>
Exclude profiles from conversion if SYSOBJH profile exists	<p>With this option, you can exclude certain types of old utility profiles from the conversion if a corresponding SYSOBJH profile already exists. You can exclude:</p> <ul style="list-style-type: none"> ■ default profiles, ■ library-specific profiles, ■ user-specific profiles, ■ user-library-specific profiles. <p>Thus you can preclude the undesired overwriting of settings in the respective existing SYSOBJH profiles.</p>

Option	Explanation
	<p>This option only affects already existing SYSOBJH profiles which would be modified by the conversion; it does not affect already existing SYSOBH profiles which would remain unchanged by the conversion nor new SYSOBJH profiles created by the conversion.</p> <p>It is recommended to first perform the CHECK function without excluding any profiles. Thus you can ascertain which existing SYSOBJH profiles would be modified automatically by the conversion - and then determine how to proceed with the conversion.</p>
Select listing type	<p>This option determines what information is displayed when the selected function is executed:</p> <ul style="list-style-type: none"> ■ D - displays <i>detailed</i> information on which setting in which old profile is converted to which setting in which SYSOBJH profile. ■ S - displays <i>summary</i> information on which SYSOBJH profiles are created and modified as a result of the conversion.

Old Profiles

After the conversion, it is recommended that the old NATLOAD/NATUNLD/SYSTRANS profiles be deleted. This is not done automatically, but has to be done manually for each old utility, using function code "DE" on the Define Utility Defaults/Templates screen (see [Defining Default Profiles](#)).

New Profiles

When a new SYSOBJH profile is created as a result of the conversion, the settings from the corresponding old NATLOAD/NATUNLD/SYSTRANS profiles are mapped to this new profile. However, the new profile may contain settings which had no counterpart in the old profiles. For such settings, the values from the SYSOBJH template/default profile will be taken.

The conversion procedure compares each old library-specific, user-specific and library-specific profile with its corresponding SYSOBJH profile. If no corresponding library-/user-/user-library-specific SYSOBJH profile exists, the SYSOBJH default profile is used for the comparison. In this case, a new library-/user-/user-library-specific SYSOBJH profile is only created if its settings were different from the default profile (because a specific profile that is identical with the default profile would be superfluous). Exception: The creation of a new user-library-specific-profile also causes a new user-specific-profile for the same user to be created, even if the latter does not differ from the default profile.

14

Protecting the Natural Development Server Environment and Applications

- Protecting the Natural Development Server Environment 246
- Protecting Natural Development Server Applications 251

This section covers the following topics:

Protecting the Natural Development Server Environment

This section describes how to protect the Natural Development Server environment with Natural Security, 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:

- [Client and Server Actions](#)
- [Map Environment and Library Selection](#)
- [Protectable Functions in the Mapped Environment](#)

Client and Server Actions

Generally, you have to distinguish between:

- Natural actions which are processed in the server environment,
- Natural actions which are only processed in the client environment.

When a Natural Development Server runs under control of Natural Security, only actions on the server can be protected by Natural Security. The conditions of use established by Natural Security which apply to a user's session on the *server* are *not* transferred to a *client* session.

Also, remember that some actions performed on a Natural Development Server client (mapped environment) generate a call to the Natural Development Server server, while others do not. Only if a client action causes an action on the Natural Development Server, this resulting server action will come under the control of Natural Security.

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 tree view in the mapped environment lists all non-empty libraries on the system file (FUSER/FNAT) assigned to the mapped environment which are accessible by the user.

When the user selects one of these libraries from the tree 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. If the execution of startup transactions is not desired,

it can be suppressed by setting the option "**NDV Startup Inactive**" (see *Library and User Preset Values* in the section *Administrator Services*).

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.

Protectable Functions in the Mapped Environment

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

- Tree-View Actions
- Transfer Operations
- Command-Line Actions
- System Commands
- Commands LIST DDM and EDIT DDM
- Menu-Bar Functions

Tree-View Actions



Note: Several of the tree-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 Tree View	Action	Controlled by
System-file node	List library	The action as such is always allowed and cannot be disallowed. For what is listed, see "Map Environment and Library Selection" above.
	Find object	<i>Client action not validated by the server.</i>
Library node	Open source	Command Restrictions (LIST command) in library security profile*.
	New source	Command Restrictions (EDIT command) and Editing Restrictions in library security profile*.
	Catall	Command Restrictions in library security profile*.
	Find object	Command Restrictions (SCAN 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.
	Cut	Option "Mo" (Move) "from library" for object type in SYSMAIN utility profile.

Location in Tree View	Action	Controlled by
	Copy	Option “Co” (Copy) “from library” for object type in SYSMAIN utility profile.
	Drag	Option “Co” (Copy) or “Mo” (Move) “from library” for object type in SYSMAIN utility profile.
	Paste / Drop	Option “Co” (Copy) or “Mo” (Move) “to library” for object type in SYSMAIN utility profile.
Group node	Open	Command Restrictions (LIST command) in library security profile*.
	New	Editing Restrictions in library security profile*.
	Catall	Command Restrictions in library security profile*.
	Find	Command Restrictions (SCAN command) in library security profile*.
	Delete	Command Restrictions in library security profile*.
	Cut	Option “Mo” (Move) “from library” for object type in SYSMAIN utility profile.
	Copy	Option “Co” (Copy) “from library” for object type in SYSMAIN utility profile.
	Drag	Option “Co” (Copy) or “Mo” (Move) “from library” for object type in SYSMAIN utility profile.
	Paste / Drop	Option “Co” (Copy) or “Mo” (Move) “to library” for object type in SYSMAIN utility profile.
Object node	Open	Editing Restrictions in library security profile*.
	List	Command 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*.
	Debug	Command Restrictions in library security profile*.
	Find	Command Restrictions (SCAN command) in library security profile*.
	Rename	Command Restrictions in library security profile*.
	Delete	Command Restrictions in library security profile*.
	Cut	Option “Mo” (Move) “from library” for object type in SYSMAIN utility profile.
	Copy	Option “Co” (Copy) “from library” for object type in SYSMAIN utility profile.
	Drag	Option “Co” (Copy) or “Mo” (Move) “from library” for object type in SYSMAIN utility profile.
	Paste / Drop	Option “Co” (Copy) or “Mo” (Move) “to 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 Tree View	Action	Controlled by
DDM node	Open	Option "List" in SYSDDM utility profile. (*)
	New	Option "Gen" in SYSDDM utility profile. (*)
	Cut	Option "Mo" (Move) "from library" for DDM in SYSMAIN 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	Option "Edit" in SYSDDM utility profile. (*)
	Stow	Option "Cat" in SYSDDM utility profile. (*)
	Cat	Option "Cat" in SYSDDM utility profile. (*)

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

Transfer Operations

Transfer operations (for example, "Move", "Copy") and delete operations of any supported Natural object are controlled by the SYSMAIN utility profiles (unless no utility profiles for SYSMAIN are defined, in which case they are controlled by the **Utilities** option in the library profile of the library processed). Exception: the transfer of DDMs is controlled by the SYSDDM utility profiles.

The following actions are controlled by the following **SYSMAIN utility profile** options and are validated by the server (except as indicated):

Action	Option in SYSMAIN Utility Profile	Corresponding Item in Context Menu
List	Li	-
Find	<i>Client action not validated by the server.</i>	-
Copy	Co	Copy
Move	Mo	Cut and Paste
Delete	De	Delete
Rename	Ren	-
Import	<i>Client action not validated by the server.</i>	-

These options can be allowed/disallowed for each type of object individually.

Command-Line Actions



Note: Some of the command-line 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.

The following actions, when entered in the Natural Studio command line, are controlled by the following Natural Security settings and are validated by the server (except as indicated):

Action	Controlled by
Edit object	Editing Restrictions in library security profile*.
List object	Command Restrictions in library security profile*.
Scratch	Option "De" (Delete) for object type in SYSMAIN utility profile.
Uncat	Option "De" (Delete) for object type in SYSMAIN utility profile.
Purge	Option "De" (Delete) for object type in SYSMAIN utility profile.
Save	Command Restrictions in library security profile*.
Cat	Command Restrictions in library security profile*.
Stow	Command Restrictions in library security profile*.
Compopt	Command Restrictions in library security profile*.
Scan	Command Restrictions in library security profile*.
Unlock	Session Option "Unlock Objects" in user security profile.

* or special link security profile

System Commands

Only Natural system commands which are processed on the server can be protected by Natural Security. Their use is controlled by the Command Restrictions in the library security profile (or special link security profile). This comprises the following system commands: AIV, CATAL, CATALOG, CHECK, CLEAR, COMPOPT, EXECUTE, GLOBALS, HELP, LIST, MAIL, PROFILE, READ, REGISTER, RETURN, RUN, SAVE, SCAN, SETUP, STOW, TEST, UNREGISTER, UPDATE, XREF.

Commands LIST DDM and EDIT DDM

If DDMs are stored on a system file specified with the Natural profile parameter FDIC or FDDM, the following applies: In the Natural Studio, the command EDIT DDM is also available from within a user-created library. This means that it is not necessary to expand the DDM node in the tree view to be able to edit a specific DDM. However, the use of the commands LIST DDM and EDIT DDM in a server environment can only be restricted via the security profile of the Natural **SYSDDM utility**.

Menu-Bar Functions

The use of the function “Development Tools > Error Messages”, invoked from the menu bar, is controlled by the SYSERR utility profiles.

The use of the function “Development Tools > Object Handler”, invoked from the menu bar, is controlled by the SYSOBJH utility profiles.

Protecting Natural Development Server Applications

This section describes how you can control access to base applications and compound applications with Natural Security. It covers the following topics:

- Application Protection
- Components of an Application Profile
- Invoking Application Maintenance
- Selecting an Application for Processing
- Adding a New Application Profile
- Copying an Application Profile
- Modifying an Application Profile
- Renaming an Application Profile
- Deleting an Application Profile
- Displaying an Application Profile

- [Linking Users to Applications](#)

Application Protection

This section covers the following topics:

- [What are Applications?](#)
- [Prerequisites](#)
- [General Concept](#)
- [Naming Conventions](#)
- [Hierarchies of Application Profiles](#)
- [Information for Predict Users](#)
- [Defining and Activating Application Security](#)

What are Applications?

Applications are *base applications* and *compound applications* which are created and maintained in the Natural Studio's application workspace and used in conjunction with the Natural Development Server.

For information on base and compound applications, please refer to the *Natural Development Server* documentation.

Unless otherwise indicated, the term “application” within the Natural Security documentation comprises both base applications and compound applications.

Prerequisites

For the protection of applications on the development server file, the following prerequisites must be met:

- The Natural Development Server must be installed at your site (as described in the *Natural Development Server* installation documentation).
- A development server file must be defined; this definition is part of the Natural Development Server installation procedure.
- The FSEC system file used must contain the application profiles “* Base Application *” and “* Compound Application *”; these two profiles are automatically created and stored on the FSEC file by both the Natural Security installation procedure and the Natural Development Server installation procedure.
- The current Natural Security session must use a development server file.

General Concept

The protection of applications is only relevant in conjunction with the Natural Development Server. If you do not use the Natural Development Server, you need not concern yourself with application protection in Natural Security.

If you use the Natural Development Server, you should use Natural Security to control the access to applications on the development server file.

By protecting an application, you control users' access to it; that is, you control whether users are allowed to read, add, modify or delete the application in the Natural Studio's application workspace. These access rights are defined in an application security profile.

Application protection in Natural Security only affects access to an application as such; it has no effect on access to the Natural programming objects contained in the libraries that may be part of the application.

Naming Conventions

Application IDs in Natural Security must conform to the application naming conventions which are defined in the Natural Development Server. Natural Security will check if they do.

Hierarchies of Application Profiles

The installation procedures of both Natural Security and the Natural Development Server automatically create two application security profiles with the application IDs `"* Base Application *"` and `"* Compound Application *"`. These are the basic security profiles which apply to all base applications and compound applications respectively for which no individual security profiles are defined. The default access settings in the two basic profiles are all preset to `"N"`; you can change them to suit your requirements.

The Natural Development Server naming conventions allow you to set up a hierarchy of application profiles: If you create an application security profile for an application whose ID is a certain character string, the profile will apply to all applications whose IDs begin with that character string. Thus, you need not define a profile for every single application.

For example, if you defined a base application security profile with the ID `"A"`, it would apply to all base applications whose IDs begin with `"A"` (such as `"APPLX"`, `"AA01"`, `"ABC"`, `"ADE"` etc.). A profile with the ID `"ABC"` would in turn apply to, for example, `"ABCA"`, `"ABCXYZ"` etc.

Asterisk as Default Access

Such a profile hierarchy can be employed to allow/disallow at different levels the individual **default access** methods (see below) to be defined within the application profiles. If a default access in an application profile is set to `"*"`, the setting in the profile at the next higher level applies for this access method.

For example, let us assume the following base application profiles with the following settings:

ID	Settings in Profile			
* Base Application *	Read=Y	Add=Y	Modify=Y	Delete=N
A	Read=*	Add=N	Modify=*	Delete=Y
ABC	Read=*	Add=*	Modify=N	Delete=*
ABCXYZ	Read=*	Add=N	Modify=*	Delete=N

The following settings would apply:

ID	Applicable Settings	Explanation
ABCXYZ	Read is allowed.	The Read setting is determined by "* Base Application *".
	Add is not allowed.	The Add setting is determined by "ABCXYZ" itself.
	Modify is not allowed.	The Modify setting is determined at the next higher level by "ABC".
	Delete is not allowed.	The Delete setting is determined by "ABCXYZ" itself.
ABC	Read is allowed.	The Read setting is determined by "* Base Application *".
	Add is not allowed.	The Add setting is determined at the next higher level by "A".
	Modify is not allowed.	The Modify setting is determined by "ABC" itself.
	Delete is allowed.	The Delete setting is determined at the next higher level by "A".
ADE	Read is allowed.	As no security profile is defined for this application, its settings are determined by the application defined at the next higher level, that is, by "A".
	Add is not allowed.	
	Modify is allowed.	
	Delete is allowed.	
A	Read is allowed.	The Read setting is determined by "* Base Application *".
	Add is not allowed.	The Add setting is determined by "A" itself.
	Modify is allowed.	The Modify setting is determined by "* Base Application *".
	Delete is allowed.	The Delete setting is determined by "A" itself.

Information for Predict Users

The hierarchy described above corresponds to the hierarchy you can set up for Predict documentation objects. In fact, base and compound applications correspond to Predict documentation objects of type "system", subtypes "-B" and "-O" respectively (as described in the Predict documentation).

Base and compound applications also appear as Predict documentation objects types "SY-B" and "SY-O" in Natural Security's subsystem for [external objects](#). It is therefore possible to maintain application profiles either in the external objects maintenance subsystem or in the application maintenance subsystem. However, it is strongly recommended that you only use the application subsystem - but not the external objects subsystem - to maintain application profiles.

Defining and Activating Application Security

Within Natural Security, application protection is performed in two steps:

- the definition of the necessary security profiles and links,
- the activation of these profiles and links.

Definition of Security Profiles and Links

To control access to an application, you would define the following security profiles and links:

- You have to create a security profile for the *library SYSDIC* (if not already defined). In the library security profile of SYSDIC, the option “People-protected” must be set to “Y”.
- You create a *security profile for the application*, and in the profile define the access rights that are to apply to most users.
- You create a *group security profile* for all users who are to have access to applications, and add all these users to the group.
- You *link* the group to the *library SYSDIC*. Without this link, access to applications is not possible. The ID of this link is also used as session profile ID by the Natural Development Server.
- If some users are to have restricted or extended access rights, you create another group security profile for each group of users who are to have the same access rights, and add the users to the groups accordingly.
- You then *link* these other groups to the *application*, defining their access rights in the link profile.
- You also have to *link* each of these groups to the *library SYSDIC*.

Activation of Security Profiles and Links

To activate the application profiles (and related link profiles) and the protection mechanisms involved, you set the option “**Activate Security for Development Server File**” to “Y” (Administrator Services Menu > General Options). As long as this option is set to “N”, applications on the development server file are not protected against unauthorized access. It is recommended that you first create all the application profiles, group profiles and links you need, before you set this option to “Y”.

Components of an Application Profile

Components of a Base Application Profile

The following type of screen is the “basic” profile screen which appears when you invoke one of the functions Add, Copy, Modify, Display for a base application security profile:

```

14:15:03                *** NATURAL SECURITY ***                2009-07-31
                        -Modify Base Application -

                                Modified .. 2009-07-15 by SAG

Base Application ... XYZ-BASE

----- Default Access -----
Y R Read                LIBA      123   10   N
* A Add                 LIBB      123   11   P
Y M Modify              LIBC      345   33   P
N D Delete

Additional Options ... N

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

```

The individual items you may define as part of a base application security profile are explained below.

Field	Explanation
Default Access	In this column, you can allow/disallow access methods for the application object in the Natural Development Server. The possible access methods are:
	R Read the application.
	A Add the application.
	M Modify the application.
	D Delete the application.
	For each access method, you can specify one of the following values:
	Y The access method is allowed.

Field	Explanation	
	N	The access method is not allowed.
	*	The setting in the application security profile at the next higher level in the hierarchy (see Hierarchies of Application Profiles above) determines whether the access method is allowed or not.
	If you set Read access to “N”, Add, Modify and Delete access will automatically be set to “N”.	
	If you set Add, Modify or Delete access to “Y”, Read access will automatically be set to “Y”.	
	If you set Read access to “*”, you can only set Add, Modify and Delete access to “N” or “*”, but not to “Y”.	
	The access methods allowed/disallowed in the application profile will apply to all users for which no special access is defined via a link (for information on links, see Linking Users to Applications below).	
Library (display only)	<p>The IDs of the libraries which are linked to the application in the Natural Development Server.</p> <p>Up to 10 libraries are displayed at a time. If there are more, you can use PF7 and PF8 to scroll within the list of libraries.</p> <p>By pressing PF5, you can invoke Library Maintenance for the libraries displayed. (When you invoke Library Maintenance from here, it comprises only those functions relevant for the maintenance of the libraries linked to the application, and you can only maintain these libraries.)</p>	
DBID / FNR (display only)	For each library, the database ID and file number of its FUSER system file are displayed.	
NSC (display only)	For each library, information on its Natural Security definition is displayed:	
	blank	The library is not defined in Natural Security.
	N	The library is defined as not protected (that is, neither people-protected nor terminal-protected).
	P	The library is defined as people-protected or terminal-protected, or both.
	U	The library is a user's private library.
	?	The library is defined in Natural Security, but the FUSER DBID/FNR specification in the library security profile does not match the one defined in the application security profile.

Components of a Compound Application Profile

The following type of screen is the “basic” profile screen which appears when you invoke one of the functions Add, Copy, Modify, Display for a compound application security profile:

```
14:16:05                *** NATURAL SECURITY ***                2009-07-31
                        - Modify Compound Application -

                                Modified .. 2009-07-15 by SAG

Compound Application ... XYZ-COMP

----- Default Access -----
Y R Read                                Base Application          NSC
* A Add                                ABCB0012-BASE-APPL          X
Y M Modify                              ABCB0015-BASE-APPL
N D Delete                              ABCB0019A01                X

Additional Options ... N

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

The individual items you may define as part of a compound application security profile are explained below.

Field	Explanation		
Default Access	In this column, you can allow/disallow access methods for the application object in the Natural Development Server. The possible access methods are:		
	R	Read the application.	
	A	Add the application.	
	M	Modify the application.	
	D	Delete the application.	
	For each access method, you can specify one of the following values:		
	Y	The access method is allowed.	
	N	The access method is not allowed.	
	*	The setting in the application security profile at the next higher level in the hierarchy (see Hierarchies of Application Profiles above) determines whether the access method is allowed or not.	
	If you set Read access to “N”, Add, Modify and Delete access will automatically be set to “N”.		
If you set Add, Modify or Delete access to “Y”, Read access will automatically be set to “Y”.			
If you set Read access to “*”, you can only set Add, Modify and Delete access to “N” or “*”, but not to “Y”.			
The access methods allowed/disallowed in the application profile will apply to all users for which no special access is defined via a link (for information on links, see Linking Users to Applications below).			
Base Application (display only)	The IDs of the base applications which are contained in the compound application. Up to 10 base applications are displayed at a time. If there are more, you can use PF7 and PF8 to scroll within the list of base applications. By pressing PF5, you can invoke Application Maintenance for these base applications.		
NSC (display only)	X	The base application is defined in Natural Security.	
	blank	The base application is not defined in Natural Security.	

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>The following information is displayed:</p> <ul style="list-style-type: none">■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation;■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	<p>You may enter your notes on the security profile.</p>
Owners	<p>You may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain the security profile.</p> <p>If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures.</p>

For each application, the application ID, Type (“Base” or “Comp”(ound)), Status and Default Access Definition are displayed.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

Status as Selection Criterion

If you wish to list only certain applications, you can specify one of the following selection criteria in the Status field above the list (possible abbreviations are underlined):

<u>b</u> lank	All application security profiles - regardless of whether or not a corresponding application exists.
<u>A</u> LL	All applications - regardless of whether or not a corresponding security profile has been defined.
<u>D</u> EFI	Defined; that is, applications for which security profiles have been defined.
<u>U</u> NDF	Undefined; that is, applications for which no security profiles have been defined.
<u>N</u> APP	No application; that is, application security profiles for which no corresponding applications exist.

The default is *blank*; that is, all application security profiles will be listed.

Selecting a Function

The following application maintenance functions are available (possible code abbreviations are underlined):

Code	Function
<u>A</u> D	Add application
<u>C</u> O	Copy application
<u>M</u> O	Modify application
RE	Rename application
DE	Delete application
<u>D</u> I	Display application
LU	Link users to application

To invoke a function for an application, mark the application with the appropriate function code in column “Co”.

You may select various objects for various functions at the same time; that is, you can mark several applications on the screen with a function code. For each application marked, the appropriate processing screen will be displayed. You may then perform for one application after another the selected functions.

Adding a New Application Profile

To define an application to Natural Security, you create a security profile for it. You can create security profiles for:

- applications which already exist on the development server file,
- applications which do not yet exist on the development server file.

Adding a Profile for an Existing Application

On the Application Maintenance selection list, enter “UNDF” in the field “Status”.

Only those applications which have not yet been defined to Natural Security will be listed. (The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).) The application IDs displayed are those by which the applications are defined in on the development server file.

On the list, mark the application for which you wish to create a security profile with function code “AD”. The Add Application screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of an application security profile are described under [Components of an Application Profile](#) above.

When you add a new application profile, the owners specified in your own user security profile will automatically be copied into the application security profile you are creating.

Adding a Profile for a Non-Existing Application

It is possible to create application security profiles before the corresponding applications themselves are defined on the development server file.

In the command line of the Application Maintenance selection list, enter the command `ADD`.

A window will be displayed. In this window, enter an *ID* for the application. This ID must conform to the naming conventions for applications which are defined in the Natural Development Server. Natural Security will check if the ID conforms to these naming conventions. Depending on where you have invoked the window from, you may also have to specify the desired type of application (base or compound).

After you have entered a valid ID (and specified the application type), the Add Application screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of an application security profile are described under [Components of an Application Profile](#) above.

When you add a new application profile, the owners specified in your own user security profile will automatically be copied into the application security profile you are creating.

Copying an Application Profile

The Copy Application function is used to define a new application to Natural Security by creating a security profile which is identical to an already existing application security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - except the owners (these will be copied from your own user security profile into the new application security profile you are creating).

Any *links* from users to the existing application will *not* be copied.

How to Copy

On the Maintenance selection list, mark the application whose security profile you wish to duplicate with function code “CO”.

A window will be displayed. In the window, enter the ID of the new application. The ID must conform to Natural Development Server naming conventions.

After you have entered a valid ID, the new security profile will be displayed.

The individual components of the security profile you may define or modify are described under [Components of an Application Profile](#) above.

Modifying an Application Profile

The Modify Application function is used to change an existing application security profile.

On the Application Maintenance selection list, you mark the application whose security profile you wish to change with function code “MO”. The security profile of the selected application will be displayed.

The individual components of the security profile you may define or modify are described under [Components of an Application Profile](#) above.

Renaming an Application Profile

The Rename Application function allows you to change the application ID of an existing application security profile.

On the Application Maintenance selection list, you mark the application whose ID you wish to change with function code "RE". A window will be displayed in which you can enter a new ID for the application profile.

The ID must conform to Natural Development Server naming conventions.

When you rename an application security profile, the application itself will not be renamed.

Deleting an Application Profile

The Delete Application function is used to delete an existing application security profile.

On the Application Maintenance selection list, you mark the application whose profile you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete Application function and should then decide against deleting the given application security profile, leave the Delete Application window by pressing ENTER without having typed in anything.
- If you wish to delete the given application security profile, enter the application's ID in the window to confirm the deletion.

When you delete an application profile, all existing links to the application profile will also be deleted.

When you delete an application security profile, the application itself will not be deleted. The application ID will remain in the Application Maintenance selection list with the Status set to "UNDF" (undefined).

If you mark more than one application with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each application security profile with entering the application's ID, or whether all applications selected for deletion are to be deleted without this individual confirmation. Be careful not to delete an application accidentally.



Note: If an application is deleted in the Natural Development Server, the corresponding Natural Security application profile will not be deleted, but its Status will be set to "NAPP" (no application).

Displaying an Application Profile

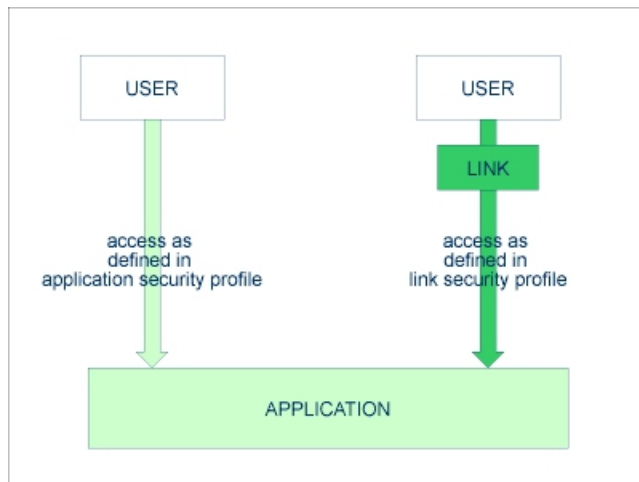
The Display Application function is used to display an existing application security profile.

On the Application Maintenance selection list, you mark the application whose security profile you wish to view with function code “DI”. The security profile of the selected application will be displayed.

The individual components of the security profile are explained under *Components of an Application Profile* above.

Linking Users to Applications

The access methods allowed/disallowed in an application security profile apply to all users who are not linked to the application. If you wish to allow an individual user more or less access methods, you can *link* the user to the application and in the link's security profile define which access methods are to be available for this particular user. This means that by using links you may define for different users different access rights to the same application.



Only users of types “Administrator”, “Person” and “Group” can be linked to an application. Administrators and Persons can be linked to an application either directly or via a Group. “Members” and “Terminals” can be linked to an application only via a Group; that is, they must be assigned to a Group, and the Group be linked to the application.

There are two functions available to establish and maintain links between users and applications:

- To link *one user* to *various applications*, use the function “Link user to applications” (which is invoked from the User Maintenance selection list).
- To link *various users* to *one application*, use the function “Link users to application” (which is invoked from the Application Maintenance selection list).

Both functions are described below.

Linking a Single User to Applications

The function “Link user to applications” is used to link one user to one or more applications.

On the User Maintenance selection list, you mark the user you wish to link with function code “LA”.

A window will be displayed. In this window, you can select the type of applications (base, compound, or both) to which you wish to link the user. In addition, the window provides the following options:

- **Start value** - Here you can enter a start value (as described in the section [Finding Your Way in Natural Security](#)) for the list of applications to be displayed.
- **Selection criterion** - N = none: all applications will be listed; L = linked: only applications to which the user is already linked will be listed; U = unlinked: only applications to which the user is not yet linked will be listed.

Then, the Link User To Applications selection list will be displayed, showing the list of applications.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

On the list, you mark the applications to which you wish to link the user.

In the “Co” column, you may mark each application with one of the following function codes (possible code abbreviations are underlined>):

Code	Function
LK	Link - The user may use the application with a special security profile to be defined for the link; the link profile will take precedence over the application profile (see below).
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display Application - The application security profile will be displayed.
D <u>L</u>	Display Link - The link security profile will be displayed.

You can mark one or more applications on the screen with a function code. For each object marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between the user and each application.

Creating a Link Security Profile

If you mark an application with “LK”, you may define the security profile for this link on the screen which will be displayed. The default settings which will appear in the link security profile are taken from the security profile of the application.

The items you may define as part of a link security profile correspond with the items you may define as part of an application security profile (see [Components of an Application Profile](#) above).

Instead of allowing/disallowing the access methods in the link security profile, you can also enter/delete the corresponding letters (R, A, M, D) in the appropriate positions in the Access column of the Link User To Applications selection list.

Moreover, you have the option to set “Activation Dates” in the link security profile; these are in analogy to the Activation Dates in a user security profile (as explained under [Components of a User Profile](#) in the section *User Maintenance*).

Modifying a Link Security Profile

To modify an existing link security profile, you mark the respective application with “LK” again on the Link User To Applications screen to invoke the link security profile screen.

Linking Multiple Users to an Application

The function “Link users to application” is used to link one or more users to one application.

On the Application Maintenance selection list, you mark the application to which you wish to link users with code “LU”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a start value (as described in the section [Finding Your Way in Natural Security](#)) for the list of users to be displayed.
- **Selection criterion** - N = none: all users will be listed; L = linked: only users which are already linked to the application will be listed; U = unlinked: only users which are not yet linked to the application will be listed.

Then, the Link Users To Application selection list will be displayed, showing the list of users.

The list includes all users of types “Group”, “Administrator” and “Person”.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

On the list, you mark the users you wish to be linked to the application.

In the “Co” column, you may mark each user with one of the following function codes (possible code abbreviations are underlined):

Code	Function
LK	Link - The user may use the application with a special security profile to be defined for the link; the link profile will take precedence over the application profile (see below).
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display User - The user security profile will be displayed.
<u>D</u> L	Display Link - The link security profile will be displayed.

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between each user and the application.

Creating a Link Security Profile

If you mark a user with “LK”, you may define the security profile for this link on the screen which will be displayed. The default settings which will appear in the link security profile are taken from the security profile of the application.

The items you may define as part of a link security profile correspond with the items you may define as part of an application security profile (see [Components of an Application Profile](#) above).

Instead of allowing/disallowing the access methods in the link security profile, you can also enter/delete the corresponding letters (R, A, M, D) in the appropriate positions in the Access column of the Link Users To Application selection list.

Moreover, you have the option to set “Activation Dates” in the link security profile; these are in analogy to the Activation Dates in a user security profile (as explained under [Components of a User Profile](#) in the section *User Maintenance*).

Modifying a Link Security Profile

To modify an existing link security profile, you mark the respective user with “LK” again on the Link Users To Application screen to invoke the link security profile screen.

15

Protecting the Natural for Eclipse Environment

- Protecting the Natural Server View for Eclipse 272
- Protecting the Eclipse Navigator View 275

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

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.
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*.

Location in Server View	Action	Controlled by
	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.

16

Protecting Natural RPC Servers and Services

■ RPC Service Requests	278
■ RPC Server Settings in Natural	278
■ RPC Server Settings in Natural Security	279
■ Validation of an RPC Service Request	280
■ Security Profiles for Natural RPC Servers	285
■ Components of an RPC Server Profile	286
■ Creating and Maintaining RPC Server Profiles	290
■ IAF Support	294
■ Other RPC-Related Features	297

This section describes the various aspects of Natural remote procedure call protection; it covers the following topics:

For general information about Natural remote procedure calls, please refer to the *Natural Remote Procedure Call* documentation.

RPC Service Requests

In a client/server environment, you can use Natural Security to protect the use of Natural remote procedure calls. You can protect Natural RPC servers as well as the way in which Natural RPC service requests issued by clients are handled.

An RPC service request is a request from a client to a Natural RPC server for a Natural subprogram to be invoked which is located in a library on the server.

When a remote `CALLNAT` is executed, and the Natural RPC Logon Option is set on the client, the following data are passed to the Natural RPC server for validation:

- the name of the subprogram to be invoked;
- the ID of the library on the server which contains the subprogram to be invoked;
- the Natural RPC user ID and password (that is, the Natural user ID and password supplied with the Natural RPC service request);
- the EntireX user ID (validation depends on Logon Option; see below).

See also the section *Using Security* in the *Natural Remote Procedure Call* documentation.

RPC Server Settings in Natural

The following Natural profile parameters on a Natural RPC server should be reviewed if the server is to be protected by Natural Security:

Profile Parameter	Explanation
RPC	<p>The settings for a Natural session which is started as a Natural RPC server are determined by the Natural profile parameter <code>RPC</code>. For a server to be protected by Natural Security, two subparameters of the <code>RPC</code> profile parameter are of particular relevance: <code>SRVNAME</code> and <code>LOGONRQ</code>.</p> <p><code>SRVNAME</code> specifies the name of the server. This is the name which has to be used as the ID for a corresponding security profile.</p>

Profile Parameter	Explanation
	<p>LOGONRQ determines whether the server is to accept only secured service requests or both public and secured service requests:</p> <ul style="list-style-type: none"> ■ A public request is a service request whose Natural RPC user ID and password are <i>not</i> validated; instead, the user ID which was used to start the server session (as contained in the Natural system variable *USER) will be used for the service request. ■ A secured request is a service request whose Natural RPC user ID and password are validated. <p>For a server to be protected by Natural Security so that only secured requests are accepted, set the LOGONRQ subparameter to "ON".</p>
FSEC	With the profile parameter FSEC, you determine the FSEC system file to be associated with the Natural RPC server.
ETID	<p>If you start the server session and specify an actual value with the profile parameter ETID, all service requests to the server will use the same specified ETID.</p> <p>If you start the server session with the profile parameter ETID=' ' (blank), no ETID can be supplied by Natural Security.</p> <p>If you start the server session with the profile parameter ETID=OFF, the ETIDs to be used by the service requests will be determined by the setting of the "Time-Stamp-Related ETID" in the security profile of the RPC server (see Components of an RPC Server Profile below). By setting this option to "Y", you can ensure an ETID handling, with appropriate database open/close processing, which allows you to uniquely identify each service request's database transactions.</p> <p>If you start a server with replicas, the ETID parameter must be set to OFF or ' ' (blank).</p>
AUTO	<p>The profile parameter AUTO (automatic logon) is only evaluated when the server session is started. For subsequent service requests to the running server, the AUTO parameter is ignored.</p> <p>If you start the server session with AUTO=OFF, you should assign a library via the profile parameter STACK=(LOGON <i>library-ID</i> ,...)</p>

RPC Server Settings in Natural Security

Generally, the Natural Security user profiles and library profiles on the FSEC system file assigned to the Natural RPC server session determine the access rights to the requested library on the server.

Specifically for the protection of Natural RPC servers, Natural Security provides the following options:

- In the security profile of a library, you can set various options which apply when the library is accessed via a Natural RPC service request. These options are described under [Natural RPC Restrictions](#) in the section *Library Maintenance*.

- You can define security profiles for Natural RPC servers, as described below in the section [Security Profiles for Natural RPC Servers](#).
- In the [Library and User Preset Values](#) section of Administrator Services, you can set various “Natural RPC Server Session Options”, which control the logon to libraries via Natural RPC service requests.

Validation of an RPC Service Request

This section covers the following topics:

- [Supported RPC Server Situations](#)
- [Security Data to Be Supplied by the Client](#)
- [Integrated Authentication Framework \(IAF\)](#)
- [Impersonation](#)
- [Validation on the Natural RPC Server](#)
- [Logon Mode](#)
- [Summary of Checks Based on Settings in Security Profiles](#)

Supported RPC Server Situations

The following situations are supported by Natural Security:

- Natural RPC server protected by Natural Security only: The Natural RPC user ID is validated.
- Natural RPC server protected by Natural Security and EntireX Security: The Natural RPC user ID and the EntireX user ID are validated.
- Natural RPC server protected by Natural Security and EntireX Security, and using the Integrated Authentication Framework (IAF): The IAF token is validated (see below).

Security Data to Be Supplied by the Client

- [Natural Clients](#)

■ Non-Natural Clients

Natural Clients

Security data are supplied by the Natural client if the Natural RPC Logon Option is set. In this case the following applies:

- The Natural RPC user ID and password to be used for the service request have to be specified via the Natural application programming interface USR1071 (contained in the library SYSEXT). To ensure that this user ID and password are available when needed, executing USR1071 should be one of the first tasks performed by an application on the client. If USR1071 is not executed and the client runs under Natural Security, the user ID and password from the Natural Security logon on the client are used instead.

If the Impersonation option is set to "A" in the RPC server security profile and the server has been started with ETID=OFF, the user ID on the client is specified via the Natural application programming interface USR4371 (contained in the library SYSEXT). In addition, USR4371 can be used to set the ETID for the service request.

- The EntireX user ID is supplied via the Natural application programming interface USR2071.
- The library ID to be used for the service request has to be specified via the Natural application programming interface USR4008 (contained in the library SYSEXT). If USR4008 is not executed, the ID of the client library in which the `CALLNAT` statement was executed is used instead.



Note: If the Natural RPC passwords used for a service request may contain special characters, make sure that the Natural character translation tables NTTABA1 and NTTABA2 on the Natural RPC server have been adjusted accordingly.

Non-Natural Clients

Please refer to the client's remote procedure call documentation for information on how to supply the required security data with an RPC service request issued by a non-Natural client to a

- Natural RPC server protected by Natural Security;
- Natural RPC server protected by Natural Security and EntireX Security;
- Natural RPC server protected by Natural Security and EntireX Security, and using the Integrated Authentication Framework (IAF).

Integrated Authentication Framework (IAF)

If a Natural RPC server is embedded in the token-based infrastructure provided by the Integrated Authentication Framework (IAF), the validation of the token which is attached to a service request passed to the Natural RPC server is performed by EntireX Security. Instead of the Natural RPC user ID and password, the IAF token - which contains the EntireX user ID - is validated during the logon to the Natural RPC server. The EntireX user ID and password are verified by EntireX Security.

Natural Security receives a successfully verified EntireX user ID. Natural Security then also uses this EntireX user ID as the Natural RPC user ID (replacing the Natural RPC user ID supplied by the client as described above). This ensures that both IDs are identical. After this point, this user ID used is considered a "trusted" Natural RPC user ID by the Natural RPC server, and is used accordingly for subsequent security checks and access authorizations.

For further information, see the section [IAF Support](#) below.

For general information on IAF, see *Integrated Authentication Framework* in the EntireX Communicator documentation. See also the section *Using the Integrated Authentication Framework* in the *Natural Remote Procedure Call* documentation.

Impersonation

For user authentication on the Natural RPC server, two modes are possible:

- validation with impersonation,
- validation without impersonation.

Impersonation assumes that access to the operating system on which a Natural RPC server is running is controlled by an SAF-compliant external security system. User authentication (verification of the Natural RPC user ID and - optionally - the password) is performed by this external security system. Impersonation means that after the authentication has been successful and the user's identity is established, any subsequent authorization checks will be performed based on this identity. This includes authorization checks for access to external resources (for example, databases or work files).

Impersonation is only possible if the Natural RPC server runs under the operating system z/OS in batch mode. Impersonation can be used if an SAF-compliant external security system is used, and user authentication is to be performed by this external security system.

Impersonation is activated by the "Impersonation" setting in the security profile of the Natural RPC server (see [Components of an RPC Server Profile](#) below).

Validation on the Natural RPC Server

Validation Without Impersonation

If impersonation is not active for the Natural RPC server, Natural Security will perform a logon to the requested library, using the Natural RPC user ID. The logon is performed according to the Natural Security logon rules and the security settings defined on the FSEC system file associated with the server.

■ With IAF:

If the Natural RPC server is embedded in the Integrated Authentication Framework (IAF), the password has been verified by EntireX, and the EntireX user ID is considered a "trusted" user ID after that point. Natural Security will replace the Natural RPC user ID with this EntireX user ID. No further password verification will be performed for this user ID.

■ Without IAF:

One check performed during the logon is based on the evaluation of the Natural RPC Restrictions > **Logon Option** in the security profile of the requested library. This option determines whether only the Natural RPC user ID or both the user ID and the password are to be verified by the Natural Security logon procedure:

- If the Logon Option is set to "N" or "E", both the user ID and the password are verified.
- If the Logon Option is set to "A" or "S", only the user ID is verified - assuming that the password has already been verified (similar to the Natural profile parameter AUTO=ON).
- In addition, if the Logon Option is set to "E" or "S", Natural Security checks if the Natural RPC user ID is identical to the EntireX user ID. If both IDs are not identical, the service request will be rejected.

After a successful logon, the requested subprogram will be executed.

If the processing of the service request includes an access to an external resource (for example, a database or work file), the external user ID which was used to start the Natural RPC server will be used to check the authorization for such an access.

Validation With Impersonation

Impersonation is only possible if the Natural RPC server runs under the operating system z/OS in batch mode. Impersonation can be used if an SAF-compliant external security system is used, and user authentication is to be performed by this external security system.

■ With IAF:

If the Natural RPC server is embedded in the Integrated Authentication Framework (IAF), the Natural server front-end passes the EntireX user ID, which in this case is identical to the Natural RPC user ID, to the external security system for verification.

■ Without IAF:

If impersonation is active for the Natural RPC server, the Natural server front-end passes the Natural RPC user ID and password (or the user ID only) to the external security system for verification.

After a successful user authentication by the external security system, Natural Security will perform a logon to the requested library. For this logon, Natural Security uses the Natural RPC user ID, but will not perform any password verification for this user. The logon is performed according to the Natural Security logon rules and the security settings defined on the FSEC system file associated with the server.

One check performed during the logon is based on the evaluation of the Natural RPC Restrictions > **Logon Option** in the security profile of the requested library: If the Logon Option is set to "E" or "S", Natural Security checks if the Natural RPC user ID is identical to the EntireX user ID. If both IDs are not identical, the RPC service request will be rejected.

After a successful logon, the requested subprogram will be executed.

If the processing of the service request includes an access to an external resource (for example, a database or work file), the Natural RPC user ID will be used to check the authorization for such an access.

Logon Mode

If you use a Natural RPC server which provides services performed by subprograms contained in a single library, you can use the **Logon Mode** option in the security profile of the Natural RPC server to improve performance. This reduces the number of database accesses to the Natural Security system file FSEC.

The library on the server is set at the start of the server session, and will remain unchanged until the end of the server session. Service requests for any other library will be rejected. If the library is unprotected (People-protected = N), the user's authorization to access the library is not checked. If the library is protected (People-protected=Y), the user's authorization to access the library is checked. After a successful check, the user's conditions of use of the library are determined by the library profile. Even if a special link exists between the user and the library, any settings in the special link profile will be ignored.



Note: When you set Logon Mode to "S" to improve performance, please be aware that other Natural Security settings also influence performance, in particular the "Logon recorded" option in user and library profiles. Moreover, the performance of ETID-triggered handling of database transactions cannot be optimized.

Summary of Checks Based on Settings in Security Profiles

This section summarizes the checks which are performed by Natural Security depending on settings in security profiles when a service request is issued to a Natural RPC server. The following steps are performed:

1. If an IAF server is used (RPC server profile > IAF Support), token validation is performed via this IAF server (see the section *IAF Support* below).
2. User authentication is performed (see the section *Validation on the Server* above).
3. RPC server profile > the **Logon Mode** option is evaluated at the start of the Natural RPC server session (see the section *Logon Mode* above).
4. Library profile > General Options > the **People-protected** option is evaluated.
5. If no IAF server is used: Library profile > Natural RPC Restrictions > the **Logon Option** is evaluated (see the section *Validation on the Server* above); Depending on its setting, it is checked whether the Natural RPC user ID is identical to the EntireX user ID.

Security Profiles for Natural RPC Servers

Default Profile

The installation procedure of Natural Security automatically creates a default security profile with the server ID `""`. This profile applies to all Natural RPC servers for which no individual security profiles are defined. You can change the settings in this default profile to suit your requirements.



Note: Should there be no default RPC server profile `""` in your FSEC system file (this may be the case because the file was not available at the installation), execute the program NSCRPCAC in the library SYSSEC. This program creates the default server profile.

Asterisk Notation for Server IDs

If you do not wish to define a security profile for every single server, you can use asterisk notation for the server ID: If you create a server security profile and choose as server ID a character string followed by an asterisk (*), the profile will apply to all servers whose IDs begin with that character string. For an individual server within such a range, you may still define an individual security profile.

For example, if you defined a server security profile with the ID `"A*"`, it would apply to all servers whose IDs begin with `"A"` (such as `"ARPC1"`, `"AA01"`, `"ABC"`, `"ADE"` etc.). A profile with the ID `"ABC*"` would in turn apply to, for example, `"ABCA"`, `"ABCXYZ"` etc.

Server Profile Components and Functions

The **components** of server security profiles and the **functions** used to create and maintain them are described below.

Some Natural Security functions use the code “RP” to represent the object type “Natural RPC servers”.

Components of an RPC Server Profile

The following type of screen is the primary profile screen which appears when you invoke one of the functions Add, Copy, Modify, Display for the security profile of a Natural RPC server:

```
11:55:00                *** NATURAL SECURITY ***                2009-07-31
                        - Modify Nat. RPC Server -

                                Modified .. 2009-07-31 by SAG

Nat. RPC Server ... RPCS01

----- Options -----
Impersonation ..... (N,Y,A): Y
Lock User ..... (N,X,*): X
Time-Stamp-Related ETID .... (N,Y): Y
Logon Mode ..... (N,S): S
IAF Support ..... .. (N,Y): N

Additional Options ... N

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

The individual items you may define as part of a Natural RPC server's security profile are explained below.

Field	Explanation
Impersonation	Impersonation is only relevant if an SAF-compliant external security system is used for user authentication. Impersonation is described above under Validation of an RPC Service Request . This option activates impersonation for the server:
	N Impersonation is not active.
	Y Impersonation is active - with verification of the user ID and the password.
	A Impersonation is active - with verification of the user ID, but not the password.
	Impersonation is only possible if the server runs under the z/OS operating system in batch mode. If it does not, the setting of this option will be ignored.
Lock User	This option only applies to libraries in whose security profiles the Lock User option (in the Natural RPC Restrictions section of the library profile) is set to "*". For these libraries, it controls the locking of users when they attempt to access these libraries on the server via Natural RPC service calls:
	N The Lock User feature is not active.
	X The Lock User feature is active for access attempts to libraries on the server via Natural RPC service calls. Once a user has reached the maximum number of logon attempts without supplying the correct password, he/she will be locked, that is, the user ID will be made "invalid". Natural Security "remembers" unsuccessful attempts across sessions: The error counters for the client user IDs which were tried out unsuccessfully are kept for access attempts in subsequent sessions, thus reducing the number of subsequent attempts with these IDs. The error counter for a user ID is only reset after a successful logon.
	* The value of the "Lock user option" in the Library And User Preset Values of Administrator Services determines whether or not the Lock User feature is active for access attempts to libraries via Natural RPC service calls.
	For details on the Lock User feature, see also the Lock User Option in the General Options section of <i>Administrator Services</i> .
Time-Stamp-Related ETID	This option only applies to secured service requests passed from Natural clients to the Natural RPC server. It determines which ETIDs are to be used for these clients during the server session:
	N The "Default ETID" as defined in the user security profile of the Natural client determines the ETID to be used.

Field	Explanation	
	Y	A time-stamp-related ETID will be generated for every service request that accesses the Natural RPC server under the control of Natural Security. The ETID is generated when the server is accessed, and will remain in effect until the service request has been processed.
	*	The setting of the ETID option in the <i>Library And User Preset Values</i> , which applies to the user security profile, will determine the ETID to be used.
	<p>If this option is set to "Y" or "*", it is recommended that the RPC server session be started with the Natural profile parameter ETID=OFF.</p> <p>For public service requests, this option has no effect; for them, the ETID of the Natural RPC server, as established at the start of the server session, is used.</p> <p>For information on time-stamp-related ETIDs, see also ETID under <i>Library And User Preset Values</i> in the <i>Administrator Services</i> section.</p>	
Logon Mode	This option can be used if only one library on the Natural RPC server is accessed:	
	N	No special logon mode applies.
	S	<p>Static Mode applies: The library on the Natural RPC server is set at the start of the server session. It will remain unchanged until the end of the server session. The server will only process service requests for this one library. Any service request with a different library ID will be rejected.</p> <p>If this option is set, the conditions of use of the library are determined by the library profile. Even if a special link exists between the user and the library, any special link profile will be ignored.</p>
	<p>Provided that the Natural RPC server provides services performed by subprograms contained in a single library, you can use this option to improve performance.</p> <p>See also <i>Validation of an RPC Service Request</i> above.</p>	
IAF Support	This option is used to activate the support of the Integrated Authentication Framework (IAF) for the server:	
	N	IAF support is not active.
	Y	<p>IAF support is active: The RPC server will use an IAF server for token validation.</p> <p>When you set this option to "Y", you will be prompted to select the IAF server to be used. If only one IAF server is defined to Natural Security or one of the IAF servers is defined as default server, this server will be used without your being prompted. The name of the IAF server assigned is displayed.</p>

Field	Explanation	
		To change the assignment, you press PF9 to select another IAF server.
	See the section IAF Support below for further information.	

Additional Options

If you either mark the field “Additional Options” with “Y” or press PF4, a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>In this window, the following information is displayed:</p> <ul style="list-style-type: none"> ■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation; ■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	In this window, you may enter your notes on the security profile.
Owners	<p>In this window, you may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain this server security profile.</p> <p>If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For information on owners and co-owners, see the section Countersignatures.</p>

Creating and Maintaining RPC Server Profiles

This section describes the functions used to create and maintain security profiles for Natural RPC servers. It covers the following topics:

- [Invoking Maintenance for Natural RPC Servers](#)
- [Adding a New Server Profile](#)
- [Selecting Existing Server Profiles for Processing](#)
- [Copying a Server Profile](#)
- [Modifying a Server Profile](#)
- [Renaming a Server Profile](#)
- [Deleting a Server Profile](#)
- [Displaying a Server Profile](#)

Invoking Maintenance for Natural RPC Servers

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark object type "Natural RPC Server" with a character or with the cursor. The Natural RPC Server Maintenance selection list will be displayed.

From this selection list, you invoke all Natural RPC server maintenance functions as described below.

Adding a New Server Profile

To define a Natural RPC server to Natural Security, you create a security profile for it.

In the command line of the Natural RPC Server Maintenance selection list, enter the command `ADD`.

A window will be displayed. In this window, enter an *ID* for the server. This ID corresponds to the server name as specified with the Natural profile parameter `RPC` (see [RPC Server Settings in Natural](#) above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under [Security Profiles for Natural RPC Servers](#) above.

After you have entered a valid ID, the Add Natural RPC Server screen will be displayed.

The individual items you may define on this screen and any additional windows that may be part of a server security profile are described under [Components of an RPC Server Profile](#) above.

When you add a new server profile, the owners specified in your own user security profile will automatically be copied into the server security profile you are creating.

Selecting Existing Server Profiles for Processing

When you invoke Natural RPC Server Maintenance, a list of all Natural RPC server profiles that have been defined to Natural Security will be displayed.

If you do not want a list of all existing profiles, but wish only certain servers to be listed, you may use the Start Value option as described in the section [Finding Your Way In Natural Security](#).

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed. In the window, mark object type "Natural RPC Server" with a character or with the cursor (and, if desired, enter a start value). The Natural RPC Server Maintenance selection list will be displayed:

```

14:49:01                *** NATURAL SECURITY ***                2009-07-31
                        - Nat. RPC Server Maintenance -

Co Nat. RPC Server                                           Message
---
*
ASERV
RPC*
RPCABC01
RPCABC02
RPSRV2112

Command ==>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
Help      Exit      Flip  -      +      Canc

```

For each server, the server ID is displayed.

The list can be scrolled as described in the section [Finding Your Way In Natural Security](#).

Selecting a Function

The following maintenance functions are available for Natural RPC server profiles (possible code abbreviations are underlined):

Code	Function
<u>C</u> O	Copy server profile
<u>M</u> O	Modify server profile
R <u>E</u>	Rename server profile
D <u>E</u>	Delete server profile
<u>D</u> I	Display server profile

To invoke a function for a server profile, mark the server with the appropriate function code in column “Co”.

You may select various server profiles for various functions at the same time; that is, you can mark several servers on the screen with a function code. For each server marked, the appropriate processing screen will be displayed. You may then perform the selected functions for one server profile after another.

Copying a Server Profile

The Copy Server Profile function is used to define a new Natural RPC server to Natural Security by creating a security profile which is identical to an already existing Natural RPC server security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - except the owners (these will be copied from your own user security profile into the new server security profile you are creating).

Any *links* from users to the existing server will *not* be copied.

How to Copy

On the Maintenance selection list, mark the server whose security profile you wish to duplicate with function code “CO”.

A window will be displayed. In the window, enter the ID of the new server. The ID corresponds to the server name as specified with the Natural profile parameter RPC (see [RPC Server Settings in Natural](#) above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under [Security Profiles for Natural RPC Servers](#) above.

After you have entered a valid ID, the new security profile will be displayed.

The individual components of the security profile you may define or modify are described under *Components of an RPC Server Profile* above.

Modifying a Server Profile

The Modify Server Profile function is used to change an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose security profile you wish to change with function code “MO”. The security profile of the selected server will be displayed.

The individual components of the security profile you may define or modify are described under *Components of an RPC Server Profile* above.

Renaming a Server Profile

The Rename function allows you to change the server ID of an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose ID you wish to change with function code “RE”. A window will be displayed in which you can enter a new ID for the server profile.

The ID corresponds to the server name as specified with the Natural profile parameter RPC (see *RPC Server Settings in Natural* above), and must conform to the naming conventions for Natural RPC servers. Asterisk notation for the server ID is possible, as described under *Security Profiles for Natural RPC Servers* above.

Deleting a Server Profile

The Delete Server Profile function is used to delete an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose profile you wish to delete with function code “DE”. A window will be displayed.

- If you have invoked the Delete function and should then decide against deleting the given server security profile, leave the Delete Server Profile window by pressing ENTER without having typed in anything.
- If you wish to delete the given server security profile, enter the server ID in the window to confirm the deletion.

If you mark more than one server profile with “DE”, a window will appear in which you are asked whether you wish to confirm the deletion of each server security profile with entering the server

ID, or whether all server profiles selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a server profile accidentally.

Displaying a Server Profile

The Display Server Profile function is used to display an existing Natural RPC server security profile.

On the Natural RPC Server Maintenance selection list, you mark the server whose security profile you wish to view with function code “DI”. The security profile of the selected server will be displayed.

The individual components of the security profile are explained under [Components of an RPC Server Profile](#) above.

IAF Support

This section describes the support of the Integrated Authentication Framework (IAF), which is a component of EntireX. It covers the following topics:

- [Using IAF Servers](#)
- [Creating and Maintaining IAF Server Security Profiles](#)
- [Components of an IAF Server Security Profile](#)

For details of IAF, see *Introduction to the Integrated Authentication Framework* in the EntireX Communicator documentation. See also the section *Using the Integrated Authentication Framework* in the *Natural Remote Procedure Call* documentation.

Using IAF Servers

If IAF is installed, a Natural RPC server can use an IAF server for token validation.

An IAF server which to be used has to be defined to Natural Security, that is, a security profile has to be created for it, as described below under *Creating and Maintaining IAF Server Security Profiles*.

In the security profile of the Natural RPC server, you activate IAF support by setting the option **IAF Support** to “Y”. When you do so, you will be prompted to select the IAF server to be used by the RPC server. If only one IAF server is defined to Natural Security or one of the IAF servers is defined as default server, this one will be used without your being prompted.

Creating and Maintaining IAF Server Security Profiles

If you press PF10 on the Administrator Services > General Options screen, a list of all IAF servers for which security profiles have been defined will be displayed. From the list, you can select an existing IAF server profile for modification or deletion, or create a new security profile for an IAF server.

To create a new IAF server security profile, you press PF4 on the IAF server selection list. The Add IAF Server screen will be displayed. The items you can define on this screen as part of an IAF server security profile are described below under *Components of an IAF Server Security Profile*.

If no IAF server profiles have been defined yet, pressing PF10 on the General Options screen will invoke the Add IAF Server screen directly for you to define the first IAF server profile.

If only one IAF server profile has been defined, pressing PF10 on the General Options screen will invoke this profile directly for modification.

The following functions are available (possible code abbreviations are underlined) on the IAF Server Maintenance selection list:

Code	Function
<u>M</u> 0	Modify IAF server profile.
<u>D</u> E	Delete IAF server profile.

To invoke a function for an IAF server profile, mark the daemon with the appropriate function code in column “Co”.

You may select various profiles for various functions at the same time; that is, you can mark several IAF servers on the screen with a function code. For each server marked, the appropriate processing screen will be displayed. You can then perform the selected functions for one profile after another.

To reset all fields in an IAF server security profile, you press PF9 on the security profile screen.

Components of an IAF Server Security Profile

The individual items you can define as part of an IAF server security profile are described below.

The items correspond to appropriate settings in EntireX, which are described in detail in the EntireX Communicator documentation.

IAF Server Identification

Field	Explanation
NSC ID of IAF server	In this field, you specify the Natural Security ID of the IAF server. This is the ID by which the IAF server is assigned to a Natural RPC server in the RPC server profile (see IAF Support under Components of an RPC Server Profile above).
Default	If you mark this field with "X", this IAF server will be used by all Natural RPC servers, unless you change the IAF server assignment in individual Natural RPC server profiles.
Description	In this field, you can enter a descriptive name for the IAF server.

IAF Configuration

Field	Explanation
Operating system	In this field, you specify the operating system of the IAF server: 1 = z/OS, 2 = UNIX/Windows.
Transport method	In this field, you specify the transport method of the IAF server: 1 = SSL, 2 = SVC.
Host name	In this field, you specify the host name of the IAF server. For SSL, this is the IP address or the DNS name. For SVC, this is the NODE specified in the attribute file of the IAF server.
Port/SVC number	If the server type is SSL, you specify the port number. If the server type is SVC, you specify the SVC number.
Verify server (Y/N)	If this field is set to "Y", the subject name in the certificate of the IAF server must match the host name of the IAF server.

SSL Parameters for z/OS (Operating system = 1)

Field	Explanation
Trust store	In this field, you specify the location of the store containing certificates of trusted Certificate Authorities (CA certificates). You specify the RACF keyring which contains the CA certificate as follows: <i>user-ID/keyring-name</i> . If you omit the <i>user-ID</i> , the keyring will be associated with RACF user ID under which the Natural RPC server is started.
Key label	In this field, you specify the label of the user certificate in the the RACF keyring which is used to authenticate the RACF user ID of the Natural RPC server to the IAF server. This value has to be specified only if VERIFY-CLIENT=YES is specified in the attribute file of the IAF server.

SSL Parameters for UNIX and Windows (Operating system = 2)

Field	Explanation
Trust store	In this field, you specify the file name location of the CA certificate store. Example: C:/Certs/ExxCACert.pem
Key store	In this field, you specify the SSL certificate; it may contain the private key. Example: MyAppCert.pem
Key file	In this field, you specify the file which contains the EntireX Broker's private key, if it is not contained in the key store. Example: MyAppKey.pem
Key password	In this field, you specify the password which is used to protect the private key and to unlock the key file (e.g. MyAppKey.pem).

Other RPC-Related Features

User Exit LOGONEX4

The Natural Security user exit LOGONEX4 is invoked by the Natural Security RPC logon program after a successful logon of a Natural RPC client to a Natural RPC server. For details, see [RPC-Related User Exit](#) in the section *User Exits*.

Password Change via RPC Service Request - User Exit USR2074

The Natural user exit USR2074, contained in the library SYSEXT, allows you to change the user password via a Natural RPC service request.

17

Protecting External Objects

■ Types of External Objects	300
■ IDs for External Objects	301
■ Components of an External Object's Security Profile	301
■ Creating and Maintaining External Object Security Profiles	304
■ Linking Users to External Objects	309

This section covers the following topics:

Types of External Objects

With Natural Security, you can control the use of various types of objects used by:

- [Predict Objects](#)
- [Other Objects](#)

The term *external objects* used in the Natural Security documentation comprises all the object types listed below.

Predict Objects

The following are Predict object types (they are described in the Predict documentation):

- documentation objects (*PRD-Docu-Object) (PO)
- external objects (*PRD-Ext-Object) (PE)
- functions (*PRD-Function) (PF)
- 3GL libraries (*PRD-3GL-Library) (PL)

The two-letter codes in parentheses are the corresponding object-type codes as used by some Natural Security functions.



Caution: For documentation objects of types “base application” and “compound application” (SY-B and SY-O), it is strongly recommended that instead of Natural Security's subsystem for external objects you use the application maintenance subsystem; see the section [Protecting Natural Development Server Applications](#)

Other Objects

The following types of objects are used by various other products (they are described in the corresponding product documentation):

- batch jobs (JB)
- datasets (DS)
- nodes (ND)
- operations (OP)
- printers (PR)
- volume serials (VS)
- VTAM applications (VT)

The two-letter codes in parentheses are the corresponding object-type codes as used by some Natural Security functions.

IDs for External Objects

IDs are used by Natural Security to identify external objects and their security profiles. The ID of an external object must be unique amongst all IDs of objects of the same type defined to Natural Security.

The length of the IDs and other naming conventions that may apply to external objects differ from object type to object type; please refer to the respective product documentation for information.

Asterisk Notation

For the ID of an external object, you can use asterisk notation: if you create a security profile for an external object and choose as ID a character string followed by an asterisk (*), the security profile will apply to all objects of that type whose IDs begin with that character string. For single objects (or ranges of objects) within such a range you may still define individual security profiles.

For example, you can create a security profile for a batch job with ID "ADAX", which will apply to batch job ADAX; moreover, you can create a security profile for a batch job with ID "ADA*", which will apply to all other batch jobs whose IDs begin with "ADA"; further, you can create a security profile for a batch job with ID "A*", which will apply to all other batch jobs whose IDs begin with "A"; and, you can also create a security profile for a batch job with ID "***", which will apply to all other batch jobs for which no individual security profiles are defined.

Components of an External Object's Security Profile

The following type of screen is the "basic" security profile screen for an external object, which appears when you invoke one of the functions Add, Copy, Modify, Display for an external object's security profile:

```

11:31:46                *** NATURAL SECURITY ***                2009-07-31
                        - Modify Dataset -

                                                Modified .. 2009-07-12 by SAG

Dataset ..... XYZ.SYS.SOURCE

----- Default Access -----

```

```
N I Info
N R Read
N A Alter
N D Delete
```

```
Additional Options ... N
```

```
Enter-PF13--PF14--PF15--PF16--PF17--PF18--PF19--PF20--PF21--PF22--PF23--PF24---
      Refr          Menu
```

This screen varies slightly from object type to object type.

The individual items you may define as part of an external object's security profile are explained below.

Default Access

In this column, you can allow/disallow general access methods for the external object. The possible access methods differ from object type to object type, as shown below:

Access to Predict Documentation Objects, External Objects and 3GL Libraries:	
R	Read
A	Add
M	Modify
D	Delete
Access to Predict Functions:	
E	Execute
Access to Batch Jobs:	
I	Display
S	Submit
A	Alter
D	Delete
Access to Datasets:	
I	Info
R	Read
A	Alter
D	Delete

Access to Predict Documentation Objects, External Objects and 3GL Libraries:	
Access to Nodes, Printers, VTAM Applications:	
U	Use
Access to Operations:	
P	Passive
A	Active
Access to Volume Serials:	
I	Info
C	Allocate
A	Alter
D	Delete

The individual access methods are the same as those described in the corresponding product documentation.

Mark with "Y" the access methods that are to be allowed; mark with "N" the access methods that are not to be allowed.

The access methods allowed/disallowed here will apply to all users for which no special access is defined via a link (for information on links, see [Linking Users to External Objects](#) below).

Additional Options

If you mark the field "Additional Options" on the basic security profile screen with "Y", a window will be displayed from which you can select the following options:

- Maintenance Information
- Security Notes
- Owners

The options for which something has already been specified or defined are marked with a plus sign (+).

You can select one or more items from the window by marking them with any character. For each item selected, an additional window will be displayed:

Additional Option	Explanation
Maintenance Information (display only)	<p>The following information is displayed:</p> <ul style="list-style-type: none">■ the date and time when the security profile was created, the ID of the ADMINISTRATOR who created it, and (if applicable) the IDs of the co-owners who countersigned for the creation;■ the date and time when the security profile was last modified, the ID of the ADMINISTRATOR who made the last modification, and (if applicable) the IDs of the co-owners who countersigned for the modification.
Security Notes	You may enter your notes on the security profile.
Owners	<p>You may enter up to eight IDs of ADMINISTRATORS. Only the ADMINISTRATORS specified here will be allowed to maintain the security profile.</p> <p>If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile.</p> <p>For each owner, the number of co-owners whose countersignatures will be required for maintenance permission may optionally be specified in the field after the ID.</p> <p>For an explanation of owners and co-owners, see the section Countersignatures.</p>

Creating and Maintaining External Object Security Profiles

This section describes the functions used to create and maintain security profiles for external objects. It covers the following topics:

- [Invoking Maintenance for External Objects](#)
- [Adding a New External Object](#)
- [Selecting Existing External Objects for Processing](#)
- [Copying an External Object](#)
- [Modifying an External Object](#)
- [Renaming an External Object](#)
- [Deleting an External Object](#)

- [Displaying an External Object](#)

Invoking Maintenance for External Objects

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark one type of external object with a character or with the cursor. The Maintenance selection list for the selected object type will be displayed.

From this selection list, you invoke all maintenance functions as described below.

Adding a New External Object

The Add External Object function is used to define external objects to Natural Security, that is, create security profiles for them.

In the command line of the external object Maintenance selection list, enter the command `ADD`.

A window will be displayed. In this window, enter an **ID** for the object.

The Add screen for the specified object type will be displayed. On this screen, you may define a security profile for the external object.

The individual items you may define on this screen and any additional windows that may be part of an external object's security profile are described under [Components of an External Object's Security Profile](#) above.

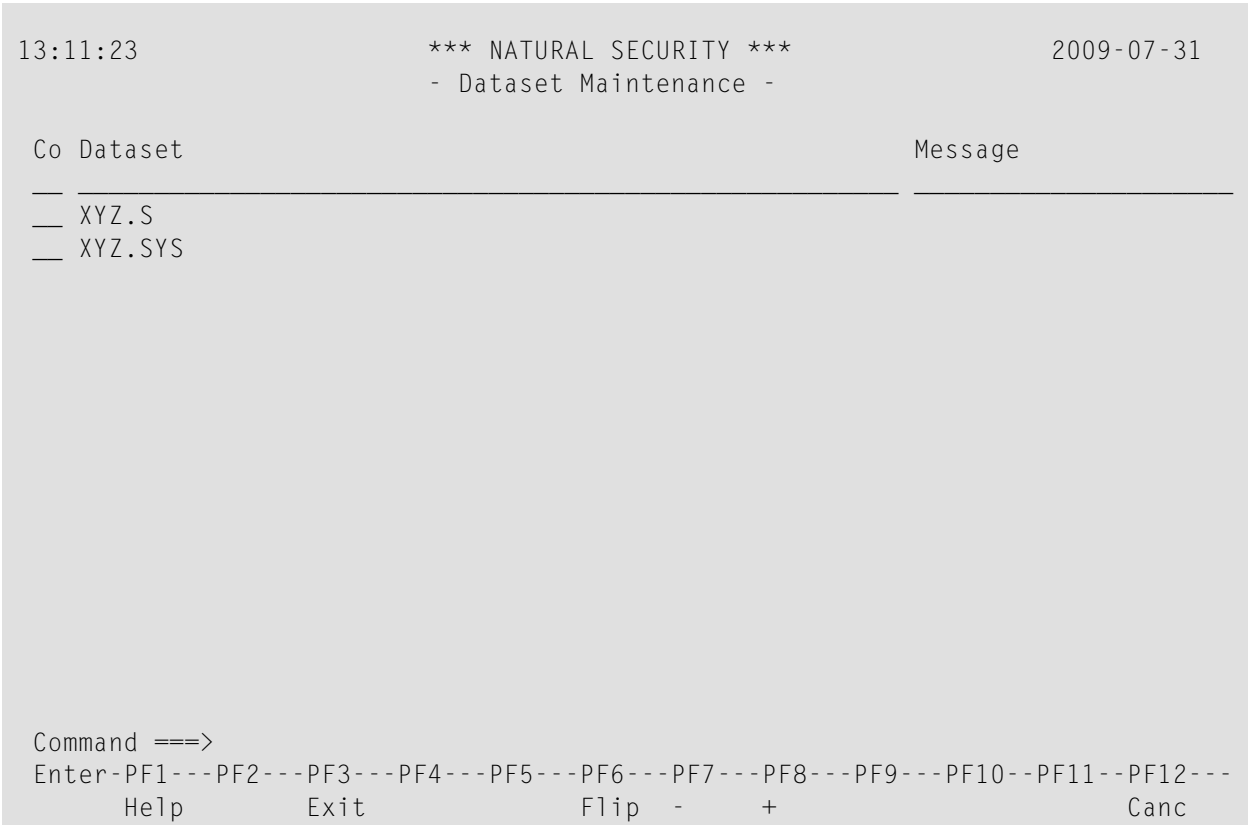
When you add a new external object, the owners specified in your own user security profile will automatically be copied into the external object's security profile you are creating.

Selecting Existing External Objects for Processing

When you invoke Maintenance for an external object, a list of all external objects of this type for which a security profile exists will be displayed.

If you do not wish to get a list of all existing external objects but would like only certain external objects to be listed, you may use the Start Value option as described in the section [Finding Your Way In Natural Security](#).

On the Main Menu, enter code "M" for “Maintenance”. A window will be displayed. In the window, mark one type of external object with a character or with the cursor (and, if desired, enter a start value). The selection list for the selected object type will be displayed; for example:



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

The following maintenance functions are available for external objects (possible code abbreviations are underlined):

Code	Function
<u>C</u> O	Copy
<u>M</u> O	Modify
RE	Rename
DE	Delete
<u>D</u> I	Display
LU	Link user

The individual functions are described below.

To invoke a specific function for an external object, mark the object with the appropriate function code in column “Co”.

You may select various objects for various functions at the same time; that is, you can mark several objects on the screen with a function code. For each object marked, the appropriate processing screen will be displayed. You may then perform for one object after another the selected functions.

Copying an External Object

The Copy function is used to define a new external object to Natural Security by creating a security profile which is identical to an already existing external object's security profile.

What is Copied?

All components of the existing security profile will be copied into the new security profile - except the owners (these will be copied from your own user security profile into the new security profile you are creating).

Any links that exist to the existing external object will *not* be copied.

How to Copy

On the Maintenance selection list, mark the external object whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In the window, enter the ID of the new external object.

The Copy screen for the external object will be displayed showing the new security profile.

This screen and any additional windows that may be part of an external object's security profile as well as the individual items you may define or modify are described under [*Components of an External Object's Security Profile*](#) above.

Modifying an External Object

The Modify function is used to change an existing external object's security profile.

On the Maintenance selection list, you mark the external object whose security profile you wish to change with function code "MO". The Modify screen for the external object will be displayed.

This screen and any additional windows that may be part of an external object's security profile as well as the individual items you may define or modify are described under [*Components of an External Object's Security Profile*](#) above.

Renaming an External Object

The Rename function allows you to change the ID of an existing external object's security profile.

On the Maintenance selection list, you mark the external object whose ID you wish to change with function code "RE". A window will be displayed in which you can enter a new ID for the external object.

Deleting an External Object

The Delete function is used to delete an existing external object's security profile.

On the Maintenance selection list, you mark the external object you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete function and should then decide against deleting the given external object's security profile, leave the Delete window by pressing `ENTER` without having typed in anything.
- If you wish to delete the given external object's security profile, enter the object's ID in the window to confirm the deletion.

When you delete an external object, all existing links to the external object will also be deleted.

If you mark more than one external object with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each external object's security profile with entering the object's ID, or whether all external objects selected for deletion are to be deleted without this individual confirmation. Be careful not to delete an external object accidentally.

Displaying an External Object

The Display function is used to display an existing external object's security profile.

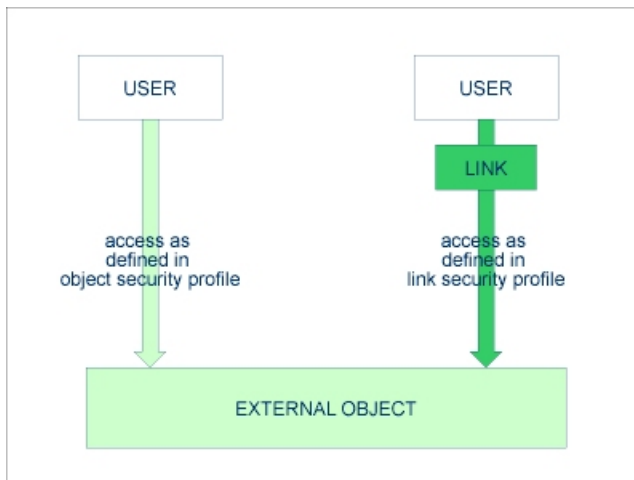
On the Maintenance selection list, you mark the external object whose security profile you wish to view with function code "DI". The Display screen for the external object will be displayed.

The items displayed on this screen and any additional windows that may be part of a external object's security profile are explained under [Components of an External Object's Security Profile](#) above.

Linking Users to External Objects

The access methods allowed/disallowed in an external object's security profile apply to all users who are not linked to the external object.

If you wish to allow an individual user more or less access methods, you can *link* the user to the external object and in the link's security profile define which access methods are to be available for this particular user. This means that by using links you may define for different users different access rights to the same external object.



Only users of types “Administrator”, “Person” and “Group” can be linked to an external object. Administrators and Persons can be linked to an external object either directly or via a Group. “Members” and “Terminals” can be linked to an external object only via a Group; that is, they must be assigned to a Group, and the Group be linked to the external object.

Two functions are available to establish and maintain links between users and external objects:

- To link *one user* to *various external objects*, use the function “Link user to external objects” (which is invoked from the User Maintenance selection list).
- To link *various users* to *one external object*, use the function “Link users to external object” (which is invoked from the Maintenance selection list of that type of external object).

Both functions are described below.

Linking a Single User to External Objects

The function “Link user to external objects” is used to link one user to one or more external objects.

On the User Maintenance selection list, you mark the user you wish to link with function code “LO”.

A window will be displayed, in which you mark with the cursor or with a character the type of external object to which you wish to link the user. In addition, the window provides the following options:

- **Start value** - Here you can enter a start value (as described in the section *Finding Your Way in Natural Security*) for the list of objects to be displayed.
- **Selection criterion** - N = none: all objects will be listed; L = linked: only objects to which the user is already linked will be listed; U = unlinked: only objects to which the user is not yet linked will be listed.

Then, the Link User To External Objects selection list will be displayed, showing the list of objects. For example:

16:04:48

*** NATURAL SECURITY ***
- Link User to Dataset -

2009-07-31

User ID AD

User Name ARTHUR DENT

Co Dataset	Access	Message
___ XYZ.S	I_____	
___ XYZ.SYS	I_A_____	

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---

HelpExitFlip - +Canc

Command ==>>>

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

On the list, you mark the external objects to which you wish to link the user.

In the “Co” column, you may mark each object with one of the following function codes (possible code abbreviations are underlined):

Code	Function
LK	Link - The user may use the external object with a special security profile to be defined for the link; the link profile will take precedence over the external object's profile (see below).
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display Object - The object's security profile will be displayed.
D <u>L</u>	Display Link - The link security profile will be displayed.

You can mark one or more objects on the screen with a function code. For each object marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between the user and each object.

Creating a Link Security Profile

If you mark an external object with “LK”, you may define the security profile for this link on the screen which will be displayed. The default settings which will appear in the link security profile are taken from the security profile of the external object.

The items you may define as part of a link security profile correspond with the items you may define as part of an external object's security profile (see [Components of an External Object's Security Profile](#) above).

Instead of allowing/disallowing the access methods in the link security profile, you can also enter/delete the corresponding letter in the appropriate position in the Access column of the Link User To External Objects selection list.

Moreover, you have the option to set “Activation Dates” in the link security profile; these are in analogy to the Activation Dates in a user security profile (as explained under [Components of a User Profile](#) in the section *User Maintenance*).

Modifying a Link Security Profile

To modify an existing link security profile, you mark the respective external object with “LK” again on the Link User To External Objects screen to invoke the link security profile screen.

Linking Multiple Users to an External Object

The function “Link users to external object” is used to link one or more users to one external object.

On the Maintenance selection list of an external object, you mark the object to which you wish to link users with code “LU”.

A window will be displayed, providing the following options:

- **Start value** - Here you can enter a start value (as described in the section *Finding Your Way in Natural Security*) for the list of users to be displayed.
- **Selection criterion** - N = none: all users will be listed; L = linked: only users already linked to the object will be listed; U = unlinked: only users not yet linked to the object will be listed.

Then, the Link Users To External Object selection list will be displayed. For example:

13:21:12*** NATURAL SECURITY ***2009-07-31

- Link Users to Dataset -

Dataset ABC.S

Default Access I

Co	User ID	User Name	Access	Message
			T IRAD	
___	AD	ARTHUR DENT	A I_A_____	
___	ADMIN1	BUNGALOW BILL	A I_AD_____	
___	ADMIN2	MARIA ALVAREZ	P I_____	
___	ADMIN3	SARA SANDOVAL	A I_____	
___	ADMIN4	ALOYSIUS PENDERGAST	A IRA_____	
___	ADMIN5	JACK SPARROW	A __AD_____	
___	ADSON	BRIAN OF NAZARETH	A I_____	
___	AGROUP	CUALQUIER GRUPO	G I__D_____	
___	HC	HAGBARD CELINE	P I_____	
___	KG	KARL GLOGAUER	P IR_____	
___	MW	MIA WALLACE	A I_____	
___	NH	NATHANIEL HAWKEYE	A __D_____	

Command ==> _____

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---

HelpExitFlip - +Canc

The list includes all users of types “Group”, “Administrator” and “Person”.

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

On the list, you may mark the users you wish to be linked to the external object.

In the “Co” column, you may mark each user with one of the following function codes (possible code abbreviations are underlined):

Code	Function
LK	Link - The user may use the external object with a special security profile to be defined for the link; the link profile will take precedence over the external object's profile (see below).
CL	Cancel - An existing link will be cancelled.
<u>D</u> I	Display User - The user security profile will be displayed.
D <u>L</u>	Display Link - The link security profile will be displayed.

You can mark one or more users on the screen with a function code. For each user marked, the selected functions will then be executed one after another. When processing is completed, a message will be displayed stating the link situation now in effect between the user and each object.

Creating a Link Security Profile

If you mark a user with “LK”, you may define the security profile for this link on the screen which will be displayed. The default settings which will appear in the link security profile are taken from the security profile of the external object.

The items you may define as part of a link security profile correspond with the items you may define as part of an external object's security profile (see [Components of an External Object's Security Profile](#) above).

Instead of allowing/disallowing the access methods in the link security profile, you can also enter/delete the corresponding letter in the appropriate position in the Access column of the Link Users To External Object selection list.

Moreover, you have the option to set “Activation Dates” in the link security profile; these are in analogy to the Activation Dates in a user security profile (as explained under [Components of a User Profile](#) in the section *User Maintenance*).

Modifying a Link Security Profile

To modify an existing link security profile, you mark the respective user/object with “LK” again on the Link Users To External Object screen to invoke the link security profile screen.

18

Mailboxes

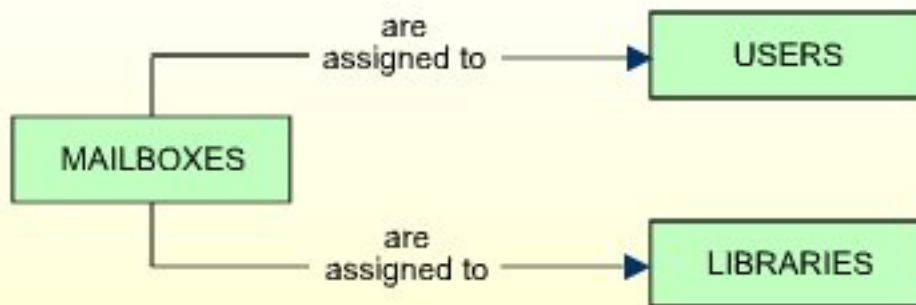
■ What is a Mailbox?	316
■ Broadcasting a Message	316
■ Receiving a Message	317
■ Mailbox ID	318
■ Components of a Mailbox Profile	318
■ Creating and Maintaining Mailbox Profiles	320

This section covers the following topics:

What is a Mailbox?

A mailbox is an information screen which may be used to broadcast messages to Natural users. It can best be described as a notice board.

Mailboxes may be assigned to users and/or to libraries.



When a user logs on to a library, the mailboxes assigned to his or her security profile, as well as the mailboxes assigned to the security profile of the library, will be displayed to the user.

You create a mailbox by defining it to Natural Security, that is, creating a security profile for it.

Broadcasting a Message

Everybody specified as a *mailer* in a mailbox security profile may use the mailbox. If a group is specified as a mailer, every user contained in the group may use the mailbox. If no mailer is specified, any user may use the mailbox.

A mailer can invoke a mailbox with the Natural system command MAIL (provided that the mailer is logged on to a library for which command mode is allowed).

Examples:

```
MAIL FUGAZI
```

This command invokes the message screen of the mailbox FUGAZI.

```
MAIL ?
```

This command displays a list of all mailboxes which the mailer may use; the mailer can then select a mailbox from the list.

Once the desired mailbox is invoked, the mailer may enter a message, add text to or delete text from an existing message, or change the “Valid from/to” dates.

Mails have access only to the message screen of a mailbox, not to the mailbox security profile. Owners may also broadcast messages, as they have access to a mailbox message screen via the security profile. However, it is only mails who may use the MAIL command.

Receiving a Message

Once a mailbox is defined, it may be assigned to users and libraries by entering the mailbox ID in the “Mailboxes” window (under “Additional Options”) of the respective user security profiles and library security profiles.

Owner logic applies to the assigning of mailboxes; that is, if owners are specified in the mailbox profile (see [Components of a Mailbox Profile](#) below), only these owners will be allowed to assign the mailbox to a user or library.

Mailboxes will be displayed to a user immediately after every successful logon to a library. The following mailboxes will be displayed to the user in the following order:

1. all mailboxes assigned to the user;
2. all mailboxes assigned to the library;
3. all mailboxes assigned to the group via which the user is logged on (if the library is people-protected and the user is linked via a group);
4. all mailboxes assigned to the user's terminal and all mailboxes assigned to the group via which the terminal is linked (if the library is terminal-protected (“Terminal-protected” set to “A”).

If one mailbox would have to be displayed more than once to a user (for example, if the same mailbox is assigned to the user's own security profile as well as to that of the group via which he/she is linked), it will only be displayed once; a repeated display will be suppressed.

The display of mailboxes cannot be suppressed by the user.

A mailbox will not be displayed

- if it is empty, that is, if it contains nothing but blanks;
- if the “Valid from” date has not yet been reached, or the “Valid to” date has passed.

Mailbox ID

Mailbox IDs are used by Natural Security to identify mailboxes and their security profiles.

A mailbox ID may be up to 8 characters long, it must start with an alphabetical character, and it must be unique amongst all mailbox IDs defined to Natural Security.

Before you start defining mailboxes, it may be advisable to conceive a logical system of mailbox IDs; this will help you to identify mailboxes easier when doing Natural Security maintenance.

Mailbox for Initial Logon

The mailbox ID “1INITIAL” serves a special purpose: if you define a mailbox with this mailbox ID, it will be displayed to every user after a successful initial logon to Natural.

The mailbox 1INITIAL need not be assigned to any user or library.

Components of a Mailbox Profile

The following screen shows an example of a mailbox security profile:

```
13:00:00                *** NATURAL SECURITY ***                2008-10-31
                        - Modify Mailbox -

Mailbox ID: MAIL2112                Created: 2007-09-14 by: SAG
Mailb.Name: MAILBOX YYZ                Modified: 2008-10-12 by: SAG
Last mailed on .. 2008-06-11 at: 12:00:58 by: IW
Valid from ..... 1999-12-31 to 2699-12-31

----- Mailbox Security Notes ----- Mailers-  -- Owners --
----- AD -----
----- HW -----
----- IW -----
-----
-----
-----
-----
-----
-----
-----
-----
-----
```

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

The individual components of a mailbox security profile are explained below.

The following items of information are entered by Natural Security:

Mailbox ID	The ID by which you have defined the mailbox to Natural Security.
Created/by	The date when the security profile was created, and the ID of the ADMINISTRATOR who created the security profile.
Modified/by	The date when the security profile was last modified, and the ID of the ADMINISTRATOR who made the latest modification.
Last mailed on/at/by	The date, time and user ID of the latest modification of the mailbox message screen and/or "Valid from/to" dates.
Valid from/to	The period of time in which the mailbox is displayed to users when they log on. These dates can be set on the mailbox message screen, not on the security profile screen.

You may specify the following items as part of a mailbox security profile:

Mailbox Name	In this field, you may specify a name for the mailbox; this name may be up to 32 characters long.
Mailbox Security Notes	In these lines, you may enter your notes on the security profile.
Mailers	You may enter up to 10 IDs of users (of any user type) who may use the mailbox to broadcast messages, that is, modify the contents of the mailbox message screen. If no mailers are specified, any user may use the mailbox.
Owners	You may enter up to 8 IDs of ADMINISTRATORs. Only the ADMINISTRATORs specified here will be allowed to maintain the mailbox security profile and assign the mailbox to users/libraries. If no owner is specified, any user of type ADMINISTRATOR may do so. For each owner, the number of co-owners whose countersignatures will be required for maintenance/assignment permission may optionally be specified in the field after the ID. For an explanation of owners and co-owners, see the section Countersignatures .

If you press PF4 on the Add Mailbox screen, the message screen of the mailbox will be displayed:

```
13:00:27          *** Mailbox Message Screen ***          2008-10-31

Mailbox ID ... MAIL2112      Valid from 2008-05-24 to 2699-12-31
Last mailed on 2008-06-11 at 12:00:58 by IW
+-----+
I THERE IS UNREST IN THE FOREST      I
I THERE IS TROUBLE WITH THE TREES    I
I FOR THE MAPLES WANT MORE SUNLIGHT  I
I AND THE OAKS IGNORE THEIR PLEAS    I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
I                                     I
+-----+
```

Valid from/to	<p>These dates may be set if a message is only relevant for a certain period of time, and the mailbox is therefore only to be displayed to users at logon within this period of time.</p> <p>If a “from” date is specified, the mailbox will only be displayed beginning on this day.</p> <p>If a “to” date is specified, the mailbox will no longer be displayed after this day.</p> <p>Any mailer (or owner) may specify these dates.</p> <p>The format in which the dates have to be specified depend on the setting of the Natural profile parameter DTFORM.</p>
---------------	--

Creating and Maintaining Mailbox Profiles

This section describes the functions used to create and maintain mailbox profiles. It covers the following topics:

- [Invoking Mailbox Maintenance](#)
- [Adding a New Mailbox](#)
- [Selecting Existing Mailboxes for Processing](#)
- [Copying a Mailbox](#)
- [Modifying a Mailbox](#)

- [Renaming a Mailbox](#)
- [Deleting a Mailbox](#)
- [Displaying a Mailbox](#)

Invoking Mailbox Maintenance

On the Main Menu, enter code "M" for "Maintenance". A window will be displayed.

In the window, mark object type "Mailbox" with a character or with the cursor. The Mailbox Maintenance selection list will be displayed.

From this selection list, you invoke all mailbox maintenance functions as described below.

Adding a New Mailbox

The Add Mailbox function is used to define new mailboxes to Natural Security, that is, create mailbox security profiles.

To add a new mailbox security profile, enter the command `ADD` in the command line of the Mailbox Maintenance selection list.

A window will be displayed. In this window, you enter a [mailbox ID](#).

The Add Mailbox screen will be displayed. On this screen you may define a security profile for the mailbox. The items you may define or specify are explained under [Components of a Mailbox Profile](#) above.

When you add a new mailbox, the owners specified in your own user security profile will automatically be copied into the mailbox security profile you are creating.

Selecting Existing Mailboxes for Processing

When you invoke Mailbox Maintenance, a list of all mailboxes that have been defined to Natural Security will be displayed.

If you do not wish to get a list of all existing mailboxes but would like only certain mailboxes to be listed, you may use the Start Value option as described in the section [Finding Your Way In Natural Security](#).

On the Main Menu, enter code "M" for "Maintenance".

A window will be displayed. In the window, mark object type "Mailbox" with a character or with the cursor (and, if desired, enter a start value).

The Mailbox Maintenance selection list will be displayed:

```

11:35:19                *** NATURAL SECURITY ***                2009-07-31
                        - Mailbox Maintenance -

Co Mailbox ID Mailbox Name                                     Message
---
___ MAILAZ      MAILAZ
___ MAILB       MAILBOX B
___ MAILF       MAIL-FINANCE
___ MAILLP      PLEASE MR POSTMAN
___ MAILLP1     CHAIN MAIL
___ MAILLP2
___ MAILSAG     MAILBOX FOR SAG
___ MAILTM
___ MAIL1
___ MAIL10      NEWS AT 10
___ MAIL11
___ MAIL12
___ MAIL13
___ MAIL14
___ MAIL2112    MAILBOX YYZ

Command ==>
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help      Exit      Flip  -      +      Cancell

```

For each mailbox, its ID and name are displayed.

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

The following mailbox maintenance functions are available (possible code abbreviations are underlined):

Code	Function
<u>C</u> O	Copy mailbox
<u>M</u> O	Modify mailbox
<u>R</u> E	Rename mailbox
<u>D</u> E	Delete mailbox
<u>D</u> I	Display mailbox

To invoke a specific function for a mailbox, you mark the mailbox with the appropriate function code in column “Co”.

You may select various mailboxes for various functions at the same time; that is, you can mark several mailboxes on the screen with a function code. For each mailbox marked, the appropriate

processing screen will be displayed. You may then perform for one mailbox after another the selected functions.

Copying a Mailbox

The Copy Mailbox function is used to define a new mailbox to Natural Security by creating a security profile which is identical to an existing mailbox security profile.

What is Copied?

All components you defined for the existing security profile will be copied into the new mailbox security profile - except the owners (these will be copied from your own user security profile into the new mailbox security profile you are creating).

How to Copy

On the Mailbox Maintenance selection list, mark the mailbox whose security profile you wish to duplicate with function code "CO".

A window will be displayed. In this window, enter the ID and the name of the "new" mailbox.

The Copy Mailbox screen will be displayed showing the new security profile.

The components of the security profile you may define or modify are explained under [Components of a Mailbox Profile](#) above.

Modifying a Mailbox

The Modify Mailbox function is used to change an existing mailbox security profile.

On the Mailbox Maintenance selection list, mark the mailbox whose security profile you wish to change with function code "MO".

The Modify Mailbox screen will be displayed. On this screen you may modify the mailbox's security profile. The items you may define or modify are explained under [Components of a Mailbox Profile](#) above.

Renaming a Mailbox

The Rename Mailbox function allows you to change the mailbox ID of an existing mailbox security profile.

On the Mailbox Maintenance selection list, you mark the mailbox whose ID you wish to change with function code "RE". A window will be displayed in which you can enter a new ID for the mailbox (and, optionally, change its name).

Deleting a Mailbox

The Delete Mailbox function is used to delete an existing mailbox.

On the Mailbox Maintenance selection list, mark the mailbox you wish to delete with function code "DE". A window will be displayed.

- If you have invoked the Delete Mailbox function and should then decide against deleting the given mailbox, leave the Delete Mailbox window by pressing `ENTER` without having typed in anything.
- If you wish to delete the given mailbox, enter the mailbox ID in the window to confirm the deletion.

When you delete a mailbox, the mailbox ID will simultaneously be deleted from the security profiles of the users and libraries it has been assigned to.

If you mark more than one mailbox with "DE", a window will appear in which you are asked whether you wish to confirm the deletion of each mailbox with entering the mailbox ID, or whether all mailboxes selected for deletion are to be deleted without this individual confirmation. Be careful not to delete a mailbox accidentally.

Displaying a Mailbox

The Display Mailbox function is used to view an existing mailbox security profile.

On the Mailbox Maintenance selection list, mark the mailbox you wish to be displayed with function code "DI".

The Display Mailbox screen will be displayed, showing the security profile of the selected mailbox.

The individual components of the security profile are explained under [*Components of a Mailbox Profile*](#) above.

To view the message screen of the mailbox, press `PF4` on the Display Mailbox screen.

19

Retrieval

▪ Purpose of Retrieval Functions	326
▪ Invoking Retrieval Functions	326
▪ Cross-Reference User	327
▪ Cross-Reference Library	328
▪ Cross-Reference File	328
▪ Cross-Reference Utility	329
▪ Cross-Reference Application	329
▪ Cross-Reference External Object	329
▪ Cross-Reference Mailbox	330
▪ Retrieval in Batch Mode - Program RETRIEVE	330

This section covers the following topics:

Purpose of Retrieval Functions

The Retrieval subsystem of Natural Security may be used to retrieve information on the objects defined to Natural Security and on the existing relationships between these objects. It allows you to review the existing security profile definitions and their effects.

With Retrieval, you cannot do any Natural Security maintenance; you may only look at things.

Invoking Retrieval Functions

On the Main Menu, you enter code "R" for "Retrieval".

A window will be displayed. In the window, you mark an object type with a character or with the cursor (and, if you wish, use the Start Value and Type/Status options as described in the section *Finding Your Way In Natural Security*).

The selection list for that object type will be displayed.

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

From the list, you can invoke the following retrieval functions (possible code abbreviations are underlined):

Code	Function	Explanation
<u>D</u> I	Display	These functions are the same as those described in the appropriate maintenance sections for each object type.
<u>X</u> R	Cross-Reference	These functions are described below for each object type.

To invoke a specific function for an object, you mark the object with the appropriate function code in column "Co" on the selection list.

You may select various objects for various functions at the same time; that is, you can mark several objects on the screen with a function code. For each object marked, the appropriate processing screen will be displayed. You may then perform for one object after another the selected functions.

Cross-Reference User

This function allows you to obtain the following information:

- a list of all base and compound applications to which a user is linked;
- a list of all libraries available to a user;
- a list of all DDMs/files a user's private library is linked to;
- a list of all groups a user belongs to;
- a list of all users contained in a given group;
- a list of all security profiles owned by a user;
- a list of all DDM/file security profiles where the user is "DDM Modifier";
- a list of all external objects to which a user is linked;
- the user-specific functional security specifications for the command processors for which functional security is defined for the user.
- a list of all utility profiles defined for a user.

On the User Retrieval selection list, you mark the user whose security profile you wish to cross-reference with function code "XR".

A window will be displayed, in which you can select one or more of the following items by marking them with any character:

Applications	Displays a list of all base and compound applications to which the user is linked.
Libraries	Displays a list of all libraries available to the user.
Linked Libraries	Displays a list of all libraries to which the user is linked (directly or via a group).
DDMs / Files	Displays a list of all DDMs to which the user's private library is linked.
Groups / Members	Displays a list of all groups to which the user belongs; if the user is a group, a list of all users contained in that group will be displayed.
Owned Objects	Displays a list of all security profiles of which the user is an owner.
DDM Modifier	Displays a list of all DDM/file security profiles in which the user is specified as "DDM Modifier".
External Objects	Displays a list of all external objects to which the user is linked.
Command Processors	Displays the functional security specifications for each command processor for which functional security is defined for the user.
Utilities	Displays a list of all user-specific and user-library specific utility profiles defined for the user.

Cross-Reference Library

This function allows you to obtain the following information:

- a list of all DDMs a library is linked to;
- a list of all users linked to a library;
- the functional security specifications for the command processors in the library.
- a list of all utility profiles defined for a library.

On the Library Retrieval selection list, you mark the library whose security profile you wish to cross-reference with function code “XR”.

A window will be displayed, in which you can select one or more of the following items by marking them with any character:

DDMs / Files	Displays a list of all DDMs to which the library is linked.
Users	Displays a list of all users who are linked to the library.
Command Processors	Displays the functional security specifications for each command processor in the library for which functional security is defined.
Utilities	Displays a list of all library-specific and user-library specific utility profiles defined for the library.

Cross-Reference File

This function is only available on mainframe computers. It allows you to ascertain which libraries are linked to a file.

On the File Retrieval selection list, you mark the file whose security profile you wish to cross-reference with function code “XR”.

A window will be displayed, in which you can select one or both of the following items by marking them with any character:

Libraries	Displays a list of all libraries that are linked to the file.
Private Libraries	Displays a list of all users whose private libraries are linked to the file.

Cross-Reference Utility

This function allows you to ascertain which utility profiles exist for a utility.

On the Utility Retrieval selection list, you mark the utility whose profiles you wish to cross-reference with function code "XR".

A window will be displayed, in which you can select one or more of the following items by marking them with any character:

Library-Specific Profiles	Displays a list of all library-specific profiles defined for this utility (as well as the utility's default profile).
User-Specific and User-Library-Specific Profiles	Displays a list of all user-specific profiles and user-library-specific profiles defined for this utility.
All Profiles	Displays a list of all user-specific profiles, library-specific profiles and user-library-specific profiles, as well as the default profile defined for this utility.

Cross-Reference Application

This function allows you to ascertain which users are linked to an application.

On the Application Retrieval selection list, you mark the application whose security profile you wish to cross-reference with function code "XR". A list of all users who are linked to the application will be displayed.

Cross-Reference External Object

This function allows you to ascertain which users are linked to an external object.

On the Retrieval selection list for a type of external object, you mark the object whose security profile you wish to cross-reference with function code "XR". A list of all users who are linked to the external object will be displayed.

Cross-Reference Mailbox

This function allows you to ascertain which users and libraries a mailbox is assigned to.

On the Mailbox Retrieval selection list, you mark the mailbox whose security profile you wish to cross-reference with function code “XR”.

A window will be displayed, in which you can select one or both of the following items by marking them with any character:

Libraries	Displays a list of all libraries to which the mailbox is assigned.
Users	Displays a list of all users to which the mailbox is assigned.

Retrieval in Batch Mode - Program RETRIEVE

You can obtain all retrieval information for all objects of a certain object type at the same time. For this purpose, the library SYSSEC provides the program RETRIEVE. This program performs the Display and Cross-Reference functions for all objects of a certain object type; that is, it shows Display and Cross-Reference information for all selected objects.

The following information can be obtained:

- Output 1: a list of all selected objects, with basic information about each object.
- Output 2: display of security profiles of the selected objects.
- Output 3: cross-reference information about the selected objects.
- Output 4: display of security profiles of special links between users and libraries.

Various input parameters allow you to restrict the functions to a certain range of objects, and to determine the sequence in which the information is to be output. The input parameters for RETRIEVE are:

- **1st Parameter:**
Object type: US for users, LI for libraries, FI for files (on mainframes only), MA for mailboxes, or the corresponding code for a type of external object.
- **2nd Parameter:**
User type (for object type US): A = Administrator, P = Person, M = Member, G = Group, T = Terminal, B = Batch user.

File status (for object type FI): PUBL = Public, ACCE = Access, PRIV = Private.

■ **3rd Parameter:**

Start value: An object name (optionally with asterisk notation) to obtain information on a certain range of objects only.

■ **4th and 5th Parameters:**

Date from/to: A range of dates to obtain information only on objects created/last modified within a specific period of time.

■ **6th Parameter:**

Function: Determines which information is output, and the output sequence:

S	Output 1.
A	Output 1, then Output 2 & 3 for one object, then Output 2 & 3 for the next object, etc.
AE	Output 1, then Output 2, 3 & 4 for one object, then Output 2, 3 & 4 for the next object, etc.
X	Output 3.
XE	Output 3 & 4 for one object, then Output 3 & 4 for the next object, etc.
D	Output 1, then Output 2 for every object.
Z	Output 1, then Output 2 for every object, then Output 3 for every object.
ZE	Output 1, then Output 2 for every object, then Output 3 for every object, then Output 4 for every object.

The program RETRIEVE is primarily intended for use in batch mode. However, by issuing the direct command RETRIEVE, you can also invoke the program online: a menu will be displayed for you to specify the selection options.

20

Countersignatures

■ Using Owners	334
■ Using Countersignatures	334
■ Groups as Owners	336
■ Groups as Co-Owners	337
■ User Security Profiles of ADMINISTRATORS	337
■ Deferred Countersigning	338
■ Inaccessible Security Profiles	340

This section covers the following topics:

Using Owners

The benefit of using *owners* for security profiles is that the work and responsibility of doing Natural Security maintenance may be distributed amongst several ADMINISTRATORS instead of resting in the hands of just one person.

This distribution may be done according to criteria of significance/sensitivity of objects, regional, branch or departmental aspects, or whatever suits your specific Natural environment.

The number of ADMINISTRATORS should be kept low, and the system by which you assign owners should be clearly structured.

It is also possible to enter a GROUP as an owner. All ADMINISTRATORS contained in the GROUP will then be authorized to maintain the security profile. (As only ADMINISTRATORS may do Natural Security maintenance anyhow, users of other user types contained in that GROUP will not be affected by this.)

Using Countersignatures

It is the Natural Security ADMINISTRATORS who control all users' access rights to libraries. The question may well be asked, "Who controls the ADMINISTRATORS?" The answer is that they can control each other. This may be achieved by the use of *countersignatures*.

A security profile may have up to 8 owners. Without countersignatures, each of these owners may modify, delete, link, or edit the security profile unhindered.

If this is not desired, the countersignatures feature may be used: next to each owner of a security profile you may enter a number (1, 2 or 3); an owner must then obtain this number of countersignatures from other owners of the security profile, before he/she can gain access to the security profile. In this way, an owner cannot execute any alterations without the knowledge and consent of other owners.

Countersignatures are given by the co-owners entering their user *passwords* on the Countersignatures screen; this screen is displayed automatically when a function is invoked that requires countersignatures from co-owners of the security profile concerned.



Note: If the **Lock User Option** is active, entering a wrong password on the Countersignatures screen may result in the user who has invoked the screen being locked.

Example of Countersignatures:

In the security profile of user IW the following owners are specified:

```

+-----OWNERS-----+
! User ID ..... IW  !
!                   !
! AD                !
! HW      + 1       !
! JC      + 2       !
!                   !
!                   !
!                   !
!                   !
!                   !
!                   !
!-----+

```

Only the three ADMINISTRATORS specified may modify the security profile.

The owner situation is the following:

- Owner AD may modify the security profile unhindered, that is, without having to obtain a countersignature from any of the other owners.
- Owner HW may only modify the security profile with the consent of one of the other owners (this need not be one specific owner but can be any one of the others).
- Owner JC may only modify the security profile with the consent of two, that is, all other owners of the security profile.
- Any other administrators cannot modify the security profile, as they are not owners of the security profile.

Let us imagine that owner HW wishes to modify the security profile of user IW. On the User Maintenance selection list, he marks user "IW" with code "MO". The Countersignatures screen will be invoked:

```

13:10:14          *** NATURAL SECURITY ***          2009-07-31
                  - Modify User -

User ID .. IW

      Group ID  User ID  Password  Added  Modified
      - - - - -  - - - - -  - - - - -  - - - - -  - - - - -
1.      AD_____  _____  On: 2001-08-13 2009-01-18
2.      JC_____  _____  13:08:15 13:09:10

```

```

3.      _____  _____  By: AD      AD
4.      _____  _____
5.      _____  _____
6.      _____  _____
7.      _____  _____
8.      _____  _____

SYSSEC5588: 1 authorized owner must enter his/her password.

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

```

All other owners of the security profile are listed on the screen. One of them must enter his/her password.

If none of the other owners are available in person, they may communicate (for example, AD may reveal his password to HW, which HW may then enter on the Countersignatures screen; AD should then change his password immediately afterwards).

Once the correct password of one co-owner (either AD or JC) has been entered, the Modify User screen with the security profile of user IW will be invoked for administrator HW to execute the intended modifications.

Groups as Owners

If GROUPs are specified as owners, the following cases may occur:

- An ADMINISTRATOR is an owner of a security profile and also contained in a GROUP which is an owner of the security profile. In this case the countersignature requirements specified for the ADMINISTRATOR him-/herself apply.
- An ADMINISTRATOR is not an owner of a security profile him-/herself, but is contained in two or more GROUPs which are owners of the security profile. In this case the countersignature requirements specified for the GROUP with the fewest countersignatures apply.

If two or more GROUPs have equally few countersignatures, their alphabetical order is decisive.

Note: In the above cases an ADMINISTRATOR may be an owner more than once. This implies that the ADMINISTRATOR may provide him-/herself with one or more of the countersignatures required.

Groups as Co-Owners

If a GROUP appears as a co-owner on the Countersignatures screen, any one of the ADMINISTRATORS contained in the GROUP may countersign.

To select one ADMINISTRATOR from a GROUP, enter a “?” in the User ID field next to the Group ID on the Countersignatures screen. A list of all ADMINISTRATORS contained in the GROUP will be displayed, from which you may select the one whose countersignature you wish to obtain.

Please note that a GROUP counts as one co-owner, and one co-owner cannot provide more than one countersignature. If, for example, two countersignatures are required, these may not both be obtained from members of the same GROUP.

However, one ADMINISTRATOR may countersign more than once if he/she appears more than once as a co-owner on the Countersignatures screen, i.e. in his/her own right and/or as a member of one or more GROUPs.

User Security Profiles of ADMINISTRATORS

When an ADMINISTRATOR wishes to create any new security profiles (that is, to use an Add or Copy function), the owner situation of his/her own security profile applies:

- If the ADMINISTRATOR's security profile has no owners assigned, he/she may create new security profiles unhindered.
- If the ADMINISTRATOR's security profile has owners assigned but these do not include the ADMINISTRATOR, he/she must obtain the countersignatures of all owners of his/her security profile, before he/she may create any new security profiles.
- If the ADMINISTRATOR is one of the owners of his/her own security profile and has a number of co-owners specified, the ADMINISTRATOR must obtain this number of countersignatures from other owners of his/her security profile, before he/she may create any new security profiles.



Caution: Owners and countersignatures should be assigned with the utmost care, as it may be difficult, if not impossible, to cancel an undesired owner/co-owner configuration. “Experimenting” with this feature can also result in your locking yourself out from access to a security profile.

Deferred Countersigning

Deferred countersigning allows you to perform a maintenance function, and obtain the required countersignature later.

This functionality is also referred to as "time-independent countersigning" (TIC).

Applicability

Deferred countersigning is possible:

- on mainframe computers;
- if the number of co-owners whose countersignature you need is 1;
- for the following maintenance functions: Add, Modify, Rename and Delete of user profiles and library profiles.

The following explanation uses the term "modify" for easier reading; however, the explanation also applies to the other functions mentioned.



Note: With the current version of Natural Security, deferred countersigning is available for the functions mentioned above. With subsequent versions, it is planned to make it available for further functions.

How Deferred Countersigning Works

When you attempt to modify a security profile and the Countersignatures screen is invoked, but none of the other owners of the security profile is available to supply his/her password, you may defer the countersigning. This means that you can proceed with your intended modification and obtain the other owner's countersignature afterwards.

To do so, you press PF5 (Defer) on the Countersignatures screen.

The security profile to be modified will be invoked, and you can make your changes to it.

When you have finished modifying the security profile, it will appear in the object maintenance selection list with an indication that a countersignature is still pending for the modification. The modification will not become active until the countersignature is provided.

Until the co-owner supplies or refuses his/her countersignature, there will be two versions of the security profile:

- the *active* unmodified version,
- a *temporary* version which includes your modifications.

On the maintenance selection list, you can perform the following functions on the security profile:

Code	Function
DI	Display the active version of the security profile.
DT	Display the temporary version of the security profile. The modifications are highlighted in it.
MT	Modify the temporary version of the security profile.
RT	Revoke the countersignature request.

The co-owner can perform the following functions on the security profile:

Code	Function
DI	Display the active version of the security profile.
DT	Display the temporary version of the security profile. The modifications are highlighted in it.
CT	Invoke the Countersignatures screen to confirm the modifications.
RT	Revoke the countersignature request.

Until the countersignature is supplied or revoked, maintenance functions other than those listed above cannot be applied to the security profile.

When the countersignature is supplied by the co-owner, the modifications will be applied, that is, the active version of the security profile will be removed, and the temporary version will become the active version.

If the countersignature request is revoked - either by yourself or the co-owner - the temporary version of the security profile will be removed, and only the active version will continue to exist. Any information concerning the request will be removed.



Note: The owner/co-owner specifications in a security profile *cannot* be changed via deferred countersigning.

Listing Profiles with Pending Countersignatures

To list only those security profiles of a specific object type for which countersignatures are pending, you enter the command `SHOW TIC` (TIC = time-independent countersigning) in the command line of the object maintenance selection list.

To revert to the normal selection-list display, you enter the command again.

Renamed and Deleted Security Profiles

If you defer the countersigning for the renaming of a security profile, the profile will appear in the object maintenance selection list under both the old ID and the new ID.

If you defer the countersigning for the deletion of a security profile, the profile will remain in the object maintenance selection list until the countersignature is supplied.

Inaccessible Security Profiles

If a security profile has become completely inaccessible - that is, if an owner/co-owner configuration has been set up which does not allow any ADMINISTRATOR to access the security profile - the Natural system command INPL can be used as a last resort to recover the security profile.

You enter the INPL command; then, on the INPL menu, you enter Code "R" and Replace option "O". In the next window, you enter the object type and the ID of the security profile to be recovered. This deletes all owner entries from the security profile.

If you use the above INPL option in batch mode, work file 1 must be the Natural Security INPL file.

Example of Batch-Mode Input for Security-Profile Recovery:

```
//CMSYNIN DD *  
R,O  
U,AD  
.
```

21

Functional Security

■ Command Processors	342
■ Functional Security for a Command Processor	342
■ Allowing/Disallowing Keywords	343
■ Defining Functional Security for a Library	343
■ Defining Functional Security for a User	347
■ Functional Security for Library SYSSEC	348

This section covers the following topics:

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 <code>SYSNCP</code> , but no functional security is defined for it.
Defined	The command processor has been created with <code>SYSNCP</code> and functional security is defined for it.
Modified	<p>The command processor has been modified with <code>SYSNCP</code> after functional security was defined for it.</p> <p>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 <i>all</i> “modified” command processors in the library, you can use the application programming interface NSCLI (function code “UC”).</p>

	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	<p>The command processor has been deleted with SYSNCP, but functional security is still defined for it.</p> <p>In this case, you should also delete the functional security for the command processor (by marking the field "Functional Security Defined" with "DE").</p>

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 ***	2009-07-31
	- 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 ***		2009-07-31	
		- 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:

```

User ID ..... ABC
Library ID ..... 
Command Processor ..... 

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

```

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*.



Caution: 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.

22 Natural Security In Batch Mode

■ General Information on Batch Mode	352
■ Logon in Batch Mode	352
■ Batch User Security Profiles	354
■ Countersignatures in Batch Mode	355

This section covers the following topics:

General Information on Batch Mode

Before you use Natural Security in batch mode, you should be familiar with the general considerations concerning the use of Natural in batch mode as described in the *Natural Operations* documentation.

Please also observe the batch-mode particularities of the underlying operating system.

If you want to process a job in batch mode under Natural Security, the Natural system variable *DEVICE must set to "BATCH".

Logon in Batch Mode

This section contains information on:

- [Logon Input Data in Batch Mode](#)
- [Password Change in Batch Mode](#)
- [Automatic Logon in Batch Mode](#)
- [Startup Transaction in Batch Mode](#)
- [Mailboxes in Batch Mode](#)

Logon Input Data in Batch Mode

When you use Natural Security in batch mode, the logon procedure is started automatically. Input for the LOGON command must be provided as follows:

On mainframes in delimiter mode (IM=D), and on all other platforms:

```
%*  
library-ID,user-ID,password
```

On mainframes in forms mode (IM=F):

```
library-ID user-ID  
%*  
password
```

In forms mode, the *library-ID* must be 8 bytes long; if it is less than 8 characters long, the remaining bytes must be filled with blanks.

The input mode on mainframes is set with the Natural profile parameter IM (which is described in the *Natural Parameter Reference* documentation).

The specification of “%*” will prevent the password from being printed.

If the logon procedure is to be initialized via dynamic parameters, the LOGON command must be specified with the profile parameter STACK as follows:

```
STACK=(LOGON library-ID user-ID password)
```

If no input data are specified for the LOGON command, the Natural batch session will be terminated.



Note: Under Windows in batch mode, the map LOGONM1 instead of the dialog box GLOGONM1 is displayed as logon screen.

Password Change in Batch Mode

To change the password in batch mode, input for the LOGON command must be provided as follows:

On mainframes for delimiter mode (IM=D), and on all other platforms:

```
%*  
library-ID,user-ID,password,new-password  
%*  
,, ,new-password
```

On mainframes for forms mode (IM=F):

```
library-ID user-ID  
%*  
password new-password  
%*  
new-password
```

For forms mode, *library-ID* and *password* must be 8 bytes long; if they are shorter, the remaining bytes must be filled with blanks. The *new-password* in the last line must be preceded by 8 blanks.

Automatic Logon in Batch Mode

If you use automatic logon (Natural profile parameter AUTO=ON) in batch mode, the value of the Natural system variable *INIT-USER will be taken as user ID. By default, *INIT-USER in batch mode contains the name of the batch job under which the Natural session. A user profile for this batch job name must be defined in Natural Security. A logon with another user ID is not possible.

On mainframe computers under z/OS, the value of *INIT-USER is determined by the parameter USERID in the Natural z/OS batch interface. Depending on the setting of this parameter, this value can be supplied by the security access control block (ACEE) of the security package being used (for example, RACF or ACF2), or by the USER parameter in the job card.

Startup Transaction in Batch Mode

When you log on to a library in batch mode, the setting of the switch “Batch execution” in the library security profile determines whether the startup transaction specified in the library security profile will be executed or not. See [Transactions](#) (under *Components of a Library Profile* in the section *Library Maintenance*) for details.

Mailboxes in Batch Mode

When you log on in batch mode, it depends on the setting of the general option “[Suppress mailboxes in batch mode](#)” (as explained in the section *Administrator Services*) whether mailboxes are displayed or not.

Batch User Security Profiles

In addition to creating security profiles for users of types “A”, “P”, “M”, “G” and “T”, you can also create user security profiles of type “B” (for “batch”). They are created in the same way as other user security profiles (see [Adding a New User](#) in the section *User Maintenance*) You can then enter the user ID of such a batch user in the field “Batch User ID” of a user security profile.

Before a batch user ID can be entered in a user security profile, a security profile for this batch user ID must have been defined.

Several users may share the same batch user ID; that is, the same batch user ID can be entered in the security profiles of several users. Thus, the same conditions of use can apply to several users in batch mode, and these conditions have to be defined only once.

A batch user ID cannot be used for a logon in online mode.

In batch mode, a user logs on with his/her “normal” user ID and password. Natural Security will then use the batch user ID specified in the user's security profile, and the conditions of use defined for that batch user ID will apply.

If no batch user ID is specified in the user's security profile, the “Privileged Groups” specified in the user's security profile will be checked (in order of entry) for a batch user ID. If none of the Privileged Groups has a batch user ID either, the user's own user ID will be used.

A batch user profile cannot be linked directly to a library, it must be linked via a GROUP; that is, it must be contained in a GROUP, and the GROUP be linked to the library.

Countersignatures in Batch Mode

Countersignatures cannot be processed in batch mode. This means that security profiles which require a countersignature for maintenance permission are excluded from batch-mode processing.

23

Transferring Security Data To Another System File

■ General Information on Security Data Transfer	358
■ Using SECULD2	359
■ Using SECLOAD	361
■ Transferring Data to Another Hardware Platform	362
■ Transferring Data in Batch Mode	363

This section describes how to transfer Natural Security data from one system file to another. It covers the following topics:

General Information on Security Data Transfer

The transfer of Natural Security data from one system file to another is only relevant if you use more than one Natural Security system file.

A Natural Security system file is specified with the Natural profile parameter FSEC (which is described in the Natural *Parameter Reference* documentation).

The library SYSSEC contains two programs for the transfer of Natural Security data from one system file to another: SECULD2 and SECLOAD:

- SECULD2 is used to unload data from one system file to a work file.
- SECLOAD is used to load the data from the work file onto the other system file.

The selection of data to be transferred is done with SECULD2. SECLOAD will always attempt to transfer the complete work file. However, SECLOAD will check whether the data to be transferred are consistent with the data already stored on the system file. Inconsistent data will not be loaded.

The programs SECULD2 and SECLOAD you use must both be of the same Natural Security version. Moreover, it is recommended that the latest available version of SECULD2 and SECLOAD be used.

An FSEC system file can be shared by all supported Natural Security versions. This means that you can continue to use an existing FSEC file and need not create a new FSEC file for a new Natural Security version. However, should you decide to use a new FSEC file for a new Natural Security version and wish to transfer existing security data to this new file, you unload/load the data using the standard SECULD2/SECLOAD transfer procedure.

Both SECULD2 and SECLOAD can only be invoked from *within* the library SYSSEC.



Note: SECULD2 is the replacement of the old unloading program SECULD.

Using SECULD2

To invoke SECULD2, you enter the command “SECULD2” in the command line of any Natural Security screen. The SECULD2 menu will be displayed.

To select the type of data to be transferred, you enter one of the following function codes on the SECULD2 menu:

Function Code	Type of Data to be Unloaded
*	All security data.
D	All security data with deletion (all data will be loaded onto the work file and be deleted from the system file).
O	Objects defined in Natural Security (users, libraries, utility profiles, etc.).
L	Links between users and objects.
F	Links between libraries and files (this function is only available on mainframes).
C	Components of library profile (this function is not available on mainframes).
P	Default profiles (user or utility profiles).

In addition to the function code, you can specify the following on the SECULD2 menu:

Transfer	With this option, you specify to which work file the selected data are to be written:	
	Y	The data will be written to Work File 1 in alphanumeric form (this is the default for non-mainframe environments). Work File 1 can be used for any form of transfer supported by SECULD2/SECLOAD.
	N	The data will be written to Work File 5 in binary form (this is the default for mainframe environments). Work File 5 can only be used if the data are to be transferred to another system file on the same hardware platform.
Object Type	<p>If you select function code “O”, “L” or “P”, you also have to specify the type of object/link to be unloaded.</p> <p>If you select function code “C”, you also have to specify the type of components (DDM profiles) to be unloaded.</p> <p>For a selection list of possible types, enter a question mark (?) in the Object Type field.</p>	
Start Value	<p>You can specify an ID to unload a certain object or range of objects.</p> <p>See also Range below.</p> <p>Start Value is not applicable to function codes “*” and “D”.</p>	
Range	This field determines how the value specified in the Start Value field is to be treated:	

	<ul style="list-style-type: none"> ■ If you leave the Range field blank, the value in the Start Value field will be treated as an actual start value; that is, the range of objects to be unloaded will begin with the one whose object ID begins with to the value specified as Start Value. ■ If you enter an asterisk (*) in the Range field, the range of objects to be unloaded will comprise only those whose object IDs begin with the value specified as Start Value. ■ If you enter a plus sign (+) in the Range field, the range of objects to be unloaded will consist only of the one whose object ID is specified as Start Value - or, in the case of links, will include only those whose object ID is specified as Start Value. 				
Link ID	<p>This field can only be used in conjunction with function code "L". You can specify a user ID to unload only links of a certain user or range of users.</p> <p>To select a range of links, you use see Range field (see below).</p>				
Range	<p>This field can only be used in conjunction with function code "L". It determines how the value specified in the Link ID field is to be treated:</p> <ul style="list-style-type: none"> ■ If you leave the Range field blank, the value in the Link ID field will be treated as an actual start value; that is, the range of links to be unloaded will begin with the one whose user ID corresponds to the value specified as Link ID. ■ If you enter an asterisk (*) in the Range field, the range of links to be unloaded will only include those whose user IDs begin with the value specified as Link ID. ■ If you enter a plus sign (+) in the Range field, the range of links to be unloaded will only include those whose user ID corresponds to the value specified as Link ID. 				
Number	<p>You may specify the number of objects to be transferred.</p> <p>(This option is not applicable to function codes "*" and "D".)</p>				
Date from/to	<p>You may specify two dates to unload only objects which were created/last modified in that period of time.</p> <p>(This option is not applicable to function code "D".)</p>				
Work File	<p>You specify the name of the work file to which the data are to be written.</p> <p>If you use Work File 5, the work-file name must end with ".sag".</p> <p>This field is not available on mainframes.</p>				
Ty	<p>The type of work file:</p> <table border="1"> <tr> <td>D</td><td>Default.</td></tr> <tr> <td>N</td><td>Entire Connection work file.</td></tr> </table> <p>This field is not available on mainframes.</p>	D	Default.	N	Entire Connection work file.
D	Default.				
N	Entire Connection work file.				

Using SECLOAD

To invoke SECLOAD, you enter the command “SECLOAD” in the command line of any Natural Security screen. You will then be prompted to make the following specifications:

Load NSC Data from Work File 1	Y	The data will be read from Work File 1 (this is the default for non-mainframe environments).
	N	The data will be read from Work File 5 (this is the default for mainframe environments).
User-Defined Conversion Table	<p>You can determine whether or not a conversion table is to be used (Y/N).</p> <p>The conversion table used is provided by the API subprogram NSCCONV, which is contained in the library SYSSEC. You can adjust the table to suit your requirements. For details, see the source of NSCCONV.</p>	
Simulate Loading	<p>This option can be used to ascertain whether all data from the work file can be loaded, before you actually load them. When this function is executed, the data are loaded into the system file, and then, upon completion of the function, immediately deleted from it again.</p> <p>When activating this function, you select what type of load report you want as a result of the simulation:</p>	
	N	Simulation not active.
	A	Simulation with load report listing All records.
	R	Simulation with load report listing only Rejected records.
	L	Simulation with load report listing only Loadable records.
Work File	<p>You specify the name of the work file from which the data are to be written.</p> <p>This field is not available on mainframes.</p>	
Type of Work File	D	Default.
	N	Entire Connection work file.
	This field is not available on mainframes.	



Note: Data which are inconsistent or which already exist on the target system file will not be loaded. To ascertain why data were not loaded, please refer to the load report.

Transferring Data to Another Hardware Platform

With SECULD2 and SECLOAD, you can also transfer security data from one hardware platform to another.

To do so, you enter a “Y” in the Transfer field of the SECULD2 menu.

By pressing PF4, you can then invoke an additional window in which you can specify the following optional parameters:

Target Environment	The operating system (as in the Natural system variable *OPSYS) of the target environment.
Target FSEC DBID/FNR	The database ID and file number of the FSEC system file to which the data are to be transferred. SECLOAD will compare these specifications with the DBID/FNR of the actual FSEC file to which the data are to be loaded: if they are not the same, the data cannot be loaded. In this way, you can prevent an uncontrolled loading of security data. Otherwise anybody who got hold of the work file, could load it anywhere.
Conversion EBCDIC-ASCII	<p>You can determine whether EBCDIC-ASCII conversion is to be performed (Y/N).</p> <p>The conversion is performed by the API subprogram NSCCONV, which is contained in the library SYSSEC. For details, see the source of NSCCONV.</p>
User-Defined Conversion Table	<p>You can determine whether or not a conversion table is to be used (Y/N).</p> <p>The conversion table used is provided by the API subprogram NSCCONV, which is contained in the library SYSSEC. You can adjust the table to suit your requirements. For details, see the source of subprogram NSCCONV.</p>

The data will then be written, in alphanumeric form, to Work File 1, from where they can be loaded with SECLOAD.



Note: When data are transferred from a mainframe platform to another platform, SECLOAD also checks if library IDs conform to the naming conventions for libraries (as described under the system command LOGON in the *Natural System Commands* documentation).

Transferring Data in Batch Mode

SECULD2/SECLOAD in Batch Mode on Mainframes

Example jobs for executing SECULD2 and SECLOAD in batch mode on mainframe computers are shown below.

Example 1 of SECULD2 Job:

In this example, all users whose IDs begin with “ADE” and who were last modified between 1st January and 10th June 2008, and the library TESTLIB will be transferred to the work file CMWKF05.

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
//*****
//ULD      EXEC PGM=NATBATnn,
//  PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//          DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKF05  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
//  DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
0,N,US,ADE,*,,,,2008-01-01,2008-06-10
0,N,LI,TESTLIB,1
.
FIN
/*
```

Example 2 of SECULD2 Job:

In this example, all users whose IDs begin with “ADE” will be transferred to the work file CMWKF01. If the “Transfer” option is specified as “Y”, the job must contain a line for additional parameters (see [Transferring Data to Another Hardware Platform](#) above). In this example, no additional parameter specifications are made (that is, they are either not specified or specified as “N”).

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
/*****
//ULD      EXEC PGM=NATBATnn,
//  PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//          DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKFO1  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
//  DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
O,Y,US,ADE,*
,,N,N
.
FIN
/*
```

Example 3 of SECULD2 Job:

In this example, all libraries whose IDs begin with “SF” will be transferred to the work file CMWKFO1. The target environment is a PC, and the database ID and file number of the target FSEC system file are 89 and 356.

```
//SECULD2 JOB DEMO,CLASS= ,MSGCLASS= ,REGION=2048K
/*****
//ULD      EXEC PGM=NATBATnn,
//  PARM='DBID=10,FNR=5,FSEC=(,8),FDIC=(,9),IM=D,MT=0,MAXCL=0,MADIO=0'
//STEPLIB  DD DISP=SHR,DSN=NATURAL.Vnn.LOAD
//          DD DISP=SHR,DSN=ADABAS.Vnn.ADALOAD
//DDCARD   DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=10,MODE=MULTI
/*
//CMPRINT  DD SYSOUT=*
//CMWKFO1  DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,
//  DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628,DEN=3),DISP=(,KEEP)
//CMSYNIN  DD *
SYSSEC,DBA,PASSWORD
SECULD2
O,Y,LI,SF,*
WNT-X86,89,356,N,N
.
FIN
/*
```

Example 1 of SECLOAD Job:

In this example, the data will be read from work file 5 (CMWKF05).

```
//SECLOAD JOB DEMO,MSGCLASS= ,CLASS= ,REGION=2048K
//*****
//LOAD EXEC PGM=NATBATnn,
// PARM='DBID=7,FNR=23,FSEC=(,24),FDIC=(,25),EJ=OFF,MT=0,IM=D,MADIO=0,MAXCL=0'
//STEPLIB DD DSN=NATURAL.Vnn.LOAD,DISP=SHR
// DD DSN=ADABAS.Vnn.ADALOAD,DISP=SHR
//CMPRINT DD SYSOUT=*
//DDCARD DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=7,MODE=MULTI
/*
//CMWKF05 DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,DISP=SHR
//CMSYNIN DD *
SYSSEC,DBA,PASSWORD
SECLOAD
N,N,N
FIN
/*
```

Example 2 of SECLOAD Job:

In this example, the data will be read from work file 1 (CMWKF01).

```
//SECLOAD JOB DEMO,MSGCLASS= ,CLASS= ,REGION=2048K
//*****
//LOAD EXEC PGM=NATBATnn,
// PARM='DBID=7,FNR=23,FSEC=(,24),FDIC=(,25),EJ=OFF,MT=0,IM=D,MADIO=0,MAXCL=0'
//STEPLIB DD DSN=NATURAL.Vnn.LOAD,DISP=SHR
// DD DSN=ADABAS.Vnn.ADALOAD,DISP=SHR
//CMPRINT DD SYSOUT=*
//DDCARD DD *
ADARUN PROGRAM=USER,SVC=249,DATABASE=7,MODE=MULTI
/*
//CMWKF01 DD UNIT=TAPE,VOL=SER=NATSEC,DSN=NSC.ULD,DISP=SHR
//CMSYNIN DD *
SYSSEC,DBA,PASSWORD
SECLOAD
Y,N,N
FIN
/*
```

SECULD2/SECLOAD in Batch Mode under UNIX and OpenVMS

To execute SECULD2 and SECLOAD in batch mode under UNIX or OpenVMS, you have to provide input in the batch-mode files as follows:

The input file assigned to CMSYNIN has to contain the following:

```
SECULD2  
FIN
```

In the input file assigned to CMOBJIN you specify the data to be transferred; for example:

```
SYSSEC,DBA,PASSWORD,,  
O,Y,US,ADE*,,,,2008-02-01,2008-02-28  
,,,N,N  
.
```

This example assumes that the session was started with AUTO=OFF. With AUTO=ON, you omit the user ID and password from the first line.

The result of the data transfer will be shown in the output file assigned to CMPRINT.

For general information, see the batch-mode section in the *Natural Operations* documentation for UNIX or OpenVMS.

24

User Exits

■ Logon-Related User Exits	368
■ RPC-Related User Exit	370
■ Other User Exits	371

This section describes the user exits available with Natural Security. It contains information on:

Logon-Related User Exits

The following logon-related user exits are available:

- LOGONEX1
- LOGONEX2
- LOGONEX3
- LOGONEX5



Note: The user exit LOGONEX4 is not related to Natural Security's regular logon handling, but is only relevant in conjunction with a logon of an RPC client to a Natural RPC server in an RPC environment. It is described under *RPC-Related User Exit* below.

General Information on Sources and Objects

LOGONEX1, LOGONEX2, LOGONEX3 and LOGONEX5 are Natural subprograms which have to be stored in the library SYSLIB to be invoked.

The sources and object modules of these user exits are available in the library SYSSEC under the names NOGONEX1, NOGONEX2, NOGONEX3 and NOGONEX5 respectively.

You can modify each of the user exits to suit your requirements. To do so, you make a copy of NOGONEX n ($n = 1, 2, 3$ or 5), store it under the name LOGONEX n , make your adjustments to it, and then copy it into SYSLIB.

To ensure that the user exits are always present in SYSLIB, Natural Security proceeds as follows: The installation procedure, after loading all modules into their respective libraries, checks whether there already is a subprogram LOGONEX n contained in SYSLIB. If there is, it will be left untouched. If there is not, the object module of NOGONEX n will automatically be copied from SYSSEC to SYSLIB and stored there under the name LOGONEX n . At the same time, this ensures that your customized versions of the user exits are not accidentally overwritten by an installation procedure.

LOGONEX1

LOGONEX1 is *always* invoked by the Natural Security logon program.

Unless modified, LOGONEX1 invokes the Natural Security logon screen (map LOGONM1 or dialog box GLOGONM1; see [Logon Screen / Logon Dialog Box](#)).

By modifying LOGONEX1 it is possible to invoke your own logon screens.

LOGONEX2

LOGONEX2 is invoked by the Natural Security logon program under any of the following conditions:

- when “#” is entered as the library ID (or is passed from LOGONEX1 as library ID);
- when no library ID has been specified for the logon and neither a default library nor a private library exists which could have been invoked (see also [Logon Without Library ID](#) in the section *Logging On*).

When LOGONEX2 is invoked, the user ID and password have already been checked and found valid by the logon program. At this point, the Natural system variable *USER contains a valid value, which may be used.

Unless modified, LOGONEX2 consists of nothing but an `END` statement. On return to the logon program, a valid library ID must be passed to the logon program, otherwise the logon will be rejected. Moreover, it is possible to return one of possibly several IDs using which a user is linked to a library.

As the user ID/password check has already established the validity of the user-specific logon data when LOGONEX2 is invoked, LOGONEX2 may be used to implement additional user-specific procedures or to request user-specific data. For example, the application programming interface [SECNOTE](#) may be invoked to read user security notes.

When the logon program invokes LOGONEX1 or LOGONEX2, it passes the parameters #USERDUMMY1 and #USERDUMMY2 to the subprograms. Both parameters are provided for your use; their format/length is A8. You may assign values to these parameters in LOGONEX1 and subsequently use these values in LOGONEX2, as they are passed without modification from one subprogram to the other.

LOGONEX3

LOGONEX3 is invoked by the Natural Security logon program under any of the following conditions:

- if there are mailboxes to be displayed;
- if at least one of the parameters #USERDUMMY1 or #USERDUMMY2, passed from LOGONEX1 or LOGONEX2 respectively, is not blank.

LOGONEX3 is invoked immediately after a successful logon and before control is passed from the logon program to the library invoked; when LOGONEX3 is invoked, logon processing is completed except for the display of the mailboxes.

If LOGONEX3 is left unmodified, it performs the subprogram calls necessary for the display of mailboxes.

You may modify LOGONEX3 for one of the following purposes:

- to suppress the display of mailboxes;
- to have non-library-specific processing to be carried out immediately after a successful logon but before any library-specific transactions are executed.

LOGONEX5

LOGONEX5 is invoked by the Natural Security logon program whenever the system command LOGOFF is executed.

RPC-Related User Exit

The user exit LOGONEX4 is a Natural subprogram which is only used in an RPC environment. It is invoked by the Natural Security RPC logon program after a successful logon of an RPC client to a Natural RPC server.



Note: The logon of an RPC client to a Natural RPC server does *not* cause any of the user exits described under *Logon-Related User Exits* (see above) to be invoked.

Invoking LOGONEX4 is always the last task performed by the logon program when all other logon processing has been completed, and before an RPC service is performed. At this time, the user ID and password have already been checked and found valid by the logon program, and the Natural system variables *USER and *LIBRARY-ID contain valid values, which may be used.

In conversational mode, the user exit is invoked when the conversation is started.

The input parameters for the user exit are the library ID and subprogram name. The output parameter of the user exit is a return code; this may be used to terminate the RPC logon with a non-zero return code. If this is the case, Natural issues error NAT1696 with reason code 10.

A sample source module for LOGONEX4 is available in the library SYSSEC under the name NOGONEX4. To invoke the user exit, its object module has to be stored under the name LOGONEX4 in the library SYSTEM on the FNAT system file assigned to the RPC server. After copying it to this library, the RPC server has to be restarted.

Once the user exit has been invoked, it remains active until the end of the RPC server session.

To deactivate the user exit, you have to first terminate the RPC server, and then remove the object LOGONEX4 from the library SYSTEM.

Do *not* remove LOGONEX4 while an RPC server session using that FNAT system file is still active, because this would make the RPC server session inoperable (error NAT0082 would be issued at the next logon to the RPC server).

Other User Exits

The library SYSSEC contains several other user exits:

- NSC XX EX1 - where XX is the object type: US = user, LI = library, DD = DDM, FI = file, or OB = external object;
- NSCUSEX2.

The object-type-specific NSC XX EX1 user exit is invoked immediately after a maintenance function for an object of the respective type has been performed.

NSCUSEX2 is invoked when you use the function **Edit Group Members** and CATALOG the changes you have made. It displays a list of the group's members, indicating which members have been added to the group and which have been removed from it.

The parameters of these user exits are not modifiable.

For details, see the source code of user exits themselves.

25

Application Programming Interfaces

■ Overview of Subprograms	374
■ Subprogram NSC---L	376
■ Subprogram NSC---P	376
■ Subprogram NSC---SP	377
■ Subprogram NSC---P	377
■ Subprogram NSCADM	378
■ Subprogram NSCCHCK	378
■ Subprogram NSCDA	379
■ Subprogram NSCDA-C	379
■ Subprogram NSCDA-P	379
■ Subprogram NSCDA-S	380
■ Subprogram NSCDAU	380
■ Subprogram NSCDAUC	380
■ Subprogram NSCDAUP	381
■ Subprogram NSCDAUS	381
■ Subprogram NSCDEF	381
■ Subprogram NSCDU	382
■ Subprogram NSCFI	382
■ Subprogram NSCLI	383
■ Subprogram NSCMA	384
■ Subprogram NSCOB	385
■ Subprogram NSCUS	386
■ Subprogram NSCUT	387
■ Subprogram NSCXLO	388
■ Subprogram NSCXR	388
■ Subprogram NSCXRIER	393
■ Subprogram NSCXRUSE	393
■ Subprogram SECNOTE	394

This section describes the application programming interfaces (APIs) available with Natural Security. It covers the following topics:

Overview of Subprograms

Natural Security provides a number of application programming interfaces (APIs), that is, subprograms which may be used to access Natural Security maintenance and retrieval functions from outside the Natural Security library SYSSEC.

Use of the subprograms is controlled by the general option **“Free Access to Functions via APIs”** (which is described in the section *Administrator Services*).

On the Main Menu, you enter code “A” for “Administrator Services”. The Administrator Services Menu will be displayed.



Note: **Access to Administrator Services** may be restricted (as explained in the section *Administrator Services*).

On the Administrator Services Menu 2, you select “Application Programming Interfaces”. A list of the interface subprograms along with examples and explanatory online texts will be displayed.

The following subprograms are available:

Subprograms for Access Verification:

Subprogram	Function
NSC---L	Check if logon to a library is allowed, and which modules in a library are available to a user.
NSCCHCK	Check if access to external object is allowed.
NSCDEF	Check if object is defined to Natural Security.

Subprograms for User Authentication:

Subprogram	Function
NSC---P	Check if password is valid.
NSC---P	Check if password is valid, and change password.
NSC---SP	Check if password is valid - in RPC server environments.

Subprograms for Administrator Services:

Subprogram	Function
NSCADM	Display General Options; process (ETID-related) logon records; remove/re-establish maintenance/retrieval sections for individual object types; display users in whose security profiles a value differs from a preset value.
NSCXLO	Display maintenance log records.

Subprograms for Object Maintenance:

Subprogram	Function
NSCFI	Maintenance functions for files.
NSCLI	Maintenance functions for libraries.
NSCMA	Maintenance functions for mailboxes.
NSCOB	Maintenance functions for external objects.
NSCUS	Maintenance functions for users.
NSCUT	Maintenance functions for utilities.

Subprograms for Retrieval:

Subprogram	Function
NSCDA	Display library security profile.
NSCDA-C	Display command restrictions of library security profile.
NSCDA-P	Display security options, security limits and session parameters of library security profile.
NSCDA-S	Display statement restrictions of library security profile.
NSCDAU	Display special link security profile.
NSCDAUC	Display command restrictions of special link security profile.
NSCDAUP	Display security options, security limits and session parameters of special link security profile.
NSCDAUS	Display statement restrictions of special link security profile.
NSCDU	Display user security profile.
NSCXR	Cross-reference functions.
NSCXRIER	Display individual logon error records.
NSCXRUSE	Display users with logon error counters and unused user IDs.
SECNOTE	Display security notes of user, library or special link security profile.
NSCFI, NSCLI, NSCMA, NSCOB, NSCUS, NSCUT	The display functions (function code "DI" - Display security profile) of these subprograms are considered to be retrieval functions.

Each subprogram that is to be used must be copied into the library in which it is to be executed, or into one of the steplib's concatenated to that library.



Note: The subprograms (with the exception of SECNOTE) cannot be invoked from any of the logon-related user exits described in the section [User Exits](#).

Subprogram NSC---L

The subprogram NSC---L is used to:

- check whether a specific user is allowed to log on to a specific library;
- ascertain which modules in a library are available to a user.

NSC---L is invoked as follows:

```
CALLNAT 'NSC---L' PAPPLID PUSERID PRC PPARAM1 PNSC-MESSAGE
```

Example programs PGM---L and PGM---LM of how to invoke subprogram NSC---L, as well as explanatory texts TXT---L and TXT---LM, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGM---L(M) and TXT---L(M).

Subprogram NSC---P

The subprogram NSC---P is used to check if the password supplied together with a user ID is valid.



Note: To perform this function in a Natural RPC server environment, is it recommended that NSC---SP (see below) be used instead.

NSC---P is invoked as follows:

```
CALLNAT 'NSC---P' PUSERID PPASSWORD PUSER_NAME PRC PNSC-MESSAGE
```

An example program PGM---P of how to invoke subprogram NSC---P, as well as an explanatory text TXT---P, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGM---P and TXT---P.



Note: For the execution of this subprogram, the general option **“Maximum Number of Logon Attempts”** applies, that is, each invalid password will be considered an unsuccessful logon attempt.

Subprogram NSC---SP

The subprogram NSC---SP is only to be used in Natural RPC server environments. On the whole, it corresponds to NSC---P (described above).

It is used to check if the password supplied together with a user ID is valid.

NSC---SP is invoked as follows:

```
CALLNAT 'NSC---SP' PUSERID PPASSWORD PLIBRARYID PUSERNAME
          PPARAM1 PRC PNSC-MESSAGE
```

An example program PGM---SP of how to invoke subprogram NSC---SP, as well as an explanatory text TXT---SP, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGM---SP and TXT---SP.



Note: For the execution of this subprogram, the general option **“Maximum Number of Logon Attempts”** applies, that is, each invalid password will be considered an unsuccessful logon attempt. In addition, Natural Security will react as if the **Lock User Option** were set to “X”, that is, it will “remember” unsuccessful logon attempts across sessions. Unlike the Lock User Option, however, the locking of user IDs will not include the user ID as contained in the Natural system variable *INIT-USER. When the maximum number of logon attempts is exceeded, the Natural RPC server session will *not* be terminated.

Subprogram NSC----P

The subprogram NSC----P is used to check if the password supplied together with a user ID is valid; in addition, it is used to change the password.

NSC----P is invoked as follows:

```
CALLNAT 'NSC----P' PUSERID PPASSWORD(*) PUSER_NAME PPARAM PRC PNSC-MESSAGE
```

An example program PGM----P of how to invoke subprogram NSC----P, as well as an explanatory text TXT----P, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGM----P and TXT----P.



Note: For the execution of this subprogram, the general option **“Maximum Number of Logon Attempts”** applies, that is, each invalid password will be considered an unsuccessful logon attempt.

Subprogram NSCADM

The subprogram NSCADM is used to:

- display the settings of General Options in Administrator Services;
- process **logon records**, which is particular relevant for ETID-related logon records;
- remove/re-establish Natural Security maintenance/retrieval sections for: base/compound application profiles and RPC server profiles.
- compare a preset value (as set in the **Library and User Preset Values**) with the the corresponding actual value in user profiles to obtain a list of all user profiles in which the value differs from the preset value.

NSCADM is invoked as follows:

```
CALLNAT 'NSCADM' NSCADM-PARM PNSC-MESSAGE
```

Example programs PGMADM_{nn} of how to invoke subprogram NSCADM, as well as explanatory texts TXTADM_{nn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMADM_{nn} and TX-TADM_{nn}.

Subprogram NSCCHK

The subprogram NSCCHK is used to check whether a specific user is allowed to access a specific external object.

NSCCHK is invoked as follows:

```
CALLNAT 'NSCCHK' PCLASSID PUSERID POBJID PACCESS-TYPE PRC PPARAM1 PNSC-MESSAGE
```

An example program PGMCHK of how to invoke subprogram NSCCHK, as well as an explanatory text TXTCHK, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMCHK and TXTCHK.

Subprogram NSCDA

The subprogram NSCDA is used to display the security profile of a library.

NSCDA is invoked as follows:

```
CALLNAT 'NSCDA' #PAPPLID #PPARM #PRC #PTYPE  
             #PPARM1 #PPARM2 #PPARM3 #PTEXT(*) PNSC-MESSAGE
```

An example program PGMDA of how to invoke subprogram NSCDA, as well as an explanatory text TXTDA, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDA and TXTDA.

Subprogram NSCDA-C

The subprogram NSCDA-C is used to display the Command Restrictions part of a library security profile.

NSCDA-C is invoked as follows:

```
CALLNAT 'NSCDA-C' #PAPPLID #PRC #PTYPE #PPARM1 PNSC-MESSAGE
```

An example program PGMDA-C of how to invoke subprogram NSCDA-C, as well as an explanatory text TXTDA-C, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDA-C and TXTDA-C.

Subprogram NSCDA-P

The subprogram NSCDA-P is used to display the Security Options, Security Limits and Session Parameters parts of a library security profile.

NSCDA-P is invoked as follows:

```
CALLNAT 'NSCDA-P' #PAPPLID #PRC #PTYPE #PPARM1 #POPRBS(*) PNSC-MESSAGE
```

An example program PGMDA-P of how to invoke subprogram NSCDA-P, as well as an explanatory text TXTDA-P, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDA-P and TXTDA-P.

Subprogram NSCDA-S

The subprogram NSCDA-S is used to display the Statement Restrictions part of a library security profile.

NSCDA-S is invoked as follows:

```
CALLNAT 'NSCDA-S' #PAPPLID #PRC #PTYPE #PPARM1 PNSC-MESSAGE
```

An example program PGMDA-S of how to invoke subprogram NSCDA-S, as well as an explanatory text TXTDA-S, are provided in source form in the library SYSSEC.

The individual `CALLNAT` parameters are explained in the source codes of PGMDA-S and TXTDA-S.

Subprogram NSCDAU

The subprogram NSCDAU is used to display the security profile of a special link.

NSCDAU is invoked as follows:

```
CALLNAT 'NSCDAU' #PAPPLID #PUSERID #PRC  
              #PPARM1 #PPARM2 #PPARM3 #PTEXT(*) PNSC-MESSAGE
```

An example program PGMDAU of how to invoke subprogram NSCDAU, as well as an explanatory text TXTDAU, are provided in source form in the library SYSSEC.

The individual `CALLNAT` parameters are explained in the source codes of PGMDAU and TXTDAU.

Subprogram NSCDAUC

The subprogram NSCDAUC is used to display the Command Restrictions part of a special link security profile.

NSCDAUC is invoked as follows:

```
CALLNAT 'NSCDAUC' #PAPPLID #PUSERID #PRC #PPARM1 PNSC-MESSAGE
```

An example program PGMDAUC of how to invoke subprogram NSCDAUC, as well as an explanatory text TXTDAUC, are provided in source form in the library SYSSEC.

The individual `CALLNAT` parameters are explained in the source codes of PGMDAUC and TXTDAUC.

Subprogram NSCDAUP

The subprogram NSCDAUP is used to display the Security Options, Security Limits and Session Parameters parts of a special link security profile.

NSCDAUP is invoked as follows:

```
CALLNAT 'NSCDAUP' #PAPPLID #PUSERID #PRC #PPARM1 #POPRBS(*) PNSC-MESSAGE
```

An example program PGMDAUP of how to invoke subprogram NSCDAUP, as well as an explanatory text TXTDAUP, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDAUP and TXTDAUP.

Subprogram NSCDAUS

The subprogram NSCDAUS is used to display the Statement Restrictions part of a special link security profile.

NSCDAUS is invoked as follows:

```
CALLNAT 'NSCDAUS' #PAPPLID #PUSERID #PRC #PPARM1 PNSC-MESSAGE
```

An example program PGMDAUS of how to invoke subprogram NSCDAUS, as well as an explanatory text TXTDAUS, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDAUS and TXTDAUS.

Subprogram NSCDEF

The subprogram NSCDEF is used to check whether a specific object is defined under Natural Security, i.e. whether a security profile for the object exists.

NSCDEF is invoked as follows:

```
CALLNAT 'NSCDEF' POBJID POBJTYPE PRC PNSC-MESSAGE
```

An example program PGMDEF of how to invoke subprogram NSCDEF, as well as an explanatory text TXTDEF, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDEF and TXTDEF.

Subprogram NSCDU

The subprogram NSCDU is used to display a user security profile.

NSCDU is invoked as follows:

```
CALLNAT 'NSCDU' #PUSERID #PPARM #PRC #PPARM1 #PPARM2 #PPARM3  
              #PTEXT(*) PNSC-MESSAGE
```

An example program PGMDU of how to invoke subprogram NSCDU, as well as an explanatory text TXTDU, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMDU and TXTDU.

Subprogram NSCFI

This subprogram is only available on mainframe computers, and it can only be applied to file security profiles. For DDM security profiles, you use the subprogram **NSCLI** (see below).

The subprogram NSCFI is used to perform maintenance/retrieval functions for file security profiles from outside of the library SYSSEC.

NSCFI is invoked as follows:

```
CALLNAT 'NSCFI' PFUNCTION PFILEID PFILEID2 PRC PPFKEY(*)  
                PPARM PPARM1 PPARM2 PTEXT(*) PNSC-MESSAGE
```

Example programs PGMFI_{nnn} of how to invoke subprogram NSCFI, as well as explanatory texts TXTFI_{nnn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMFI_{nnn} and TXTFI_{nnn}.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Function
AD	Add file
CL	Cancel link between library and file
CO	Copy file
DE	Delete file
DI	Display file
MO	Modify file (including all components of its security profile)

Code	Function
RE	Establish read-link between library and file
UP	Establish update-link between library and file

Subprogram NSCLI

The subprogram NSCLI is used to perform maintenance/retrieval functions for library security profiles from outside of library SYSSEC.

NSCLI is invoked as follows:

```
CALLNAT 'NSCLI' PFUNCTION PLIBID PLIBID2 PLIBTYPE PRC PPFKEY(*)
                PPARM PPARM1 PPARM2 PTEXT(*) PPARM3 PPARM4
                PPARM5 PPARM6 POPRB(*) PNSC-MESSAGE
```

Example programs PGMLI_{nnn} of how to invoke subprogram NSCLI, as well as explanatory texts TXTLI_{nnn}, are provided in source form in the library SYSSEC. Example programs PGMDDM_{nn} of how to invoke NSCLI with function code “MD”, as well as explanatory texts TXTDDM_{nn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMLI_{nnn}, TXTLI_{nnn}, PGMDDM_{nn} and TXTDDM_{nn}.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Function
AD	Add library
CL	Cancel link between user and library
CO	Copy library
DE	Delete library
DI	Display library
DL	Display special link between user and library
DM	Display allowed/disallowed modules
ET	Get library ID via ETID
LK	Link user to library
MD	Maintain DDM profile; see also below (this function is not available on mainframes)
MM	Modify allowed/disallowed modules
MO	Modify library (including all components of its security profile)
SL	Establish special link between user and library

Code	Function
TL	Temporarily lock link between user and library
UC	Update all “modified” command processors in the library

If PFUNCTION is filled with function code “MD”, the PSUBFUNC part of the parameter PPARM has to be filled with the code for the desired subfunction. The following subfunctions are available:

Code	Subfunction
AD	Add DDM profile
CL	Cancel link between library and DDM profile
CO	Copy DDM profile
DE	Delete DDM profile
DI	Display DDM profile
MO	Modify DDM profile
RE	Establish read-link between library and DDM profile
UP	Establish update-link between library and DDM profile

Subprogram NSCMA

The subprogram NSCMA is used to perform maintenance/retrieval functions for mailbox security profiles from outside of the library SYSSEC.

NSCMA is invoked as follows:

```
CALLNAT 'NSCMA' PFUNCTION POBJID POBJID2 PRC PPFKEY(*)  
          PPARM PPARM1 PPARM2 PTEXT1(*) PTEXT2(*) PNSC-MESSAGE
```

Example programs PGMMA_{nnn} showing how to invoke subprogram NSCMA, as well as explanatory texts TXTMA_{nnn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMMA_{nnn} and TXTMA_{nnn}.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Function
AD	Add mailbox
CO	Copy mailbox
DE	Delete mailbox
DI	Display mailbox
MO	Modify mailbox (including all components of its security profile)
RE	Rename mailbox

Subprogram NSCOB

The subprogram NSCOB is used to perform maintenance/retrieval functions for external object security profiles from outside of library SYSSEC.

NSCOB is invoked as follows:

```
CALLNAT 'NSCOB' PFUNCTION PCLASSID POBJID POBJID2 PRC PPFKEY(*)
          PPARM PPARM1 PPARM2 PTEXT(*) PNC-MESSAGE
```

Example programs PGMOB *nnn* of how to invoke subprogram NSCOB, as well as explanatory texts TXTOB *nnn*, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMOB *nnn* and TXTOB *nnn*.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Function
AD	Add external object
CL	Cancel link between user and external object
CO	Copy external object
DE	Delete external object
DI	Display external object
DL	Display link between user and external object
LK	Link user to external object
MO	Modify external object (including all components of its security profile)

Subprogram NSCUS

The subprogram NSCUS is used to perform maintenance/retrieval functions for user security profiles from outside of library SYSSEC.



Note: NSCUS cannot be used for private libraries which may be attached to user security profiles; for maintenance/retrieval of private libraries, you use subprogram [NSCLI](#).

NSCUS is invoked as follows:

```
CALLNAT 'NSCUS' PFUNCTION PUSERID PUSERID2 PRC PPFKEY(*)
          PPARM PPARM1 PPARM2 PTEXT(*) PPARM3 PPARM4 PNSC-MESSAGE
```

Example programs PGMUS_{nnn} of how to invoke subprogram NSCUS, as well as explanatory texts TXTUS_{nnn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMUS_{nnn} and TXTUS_{nnn}.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Function
AD	Add user
AM	Multiple add user
CO	Copy user
DE	Delete user
DI	Display user
EG	Edit group members
ET	Get user ID via ETID
MO	Modify user (including all components of his/her security profile)



Note: The user maintenance function “Copy User's Links” is not available via NSCUS.

For function code “EG”, the following subfunctions are available:

Code	Subfunction
AD	Add users to a group
DE	Delete users from a group
LI	List group members

Subprogram NSCUT

The subprogram NSCUT is used to perform maintenance/retrieval functions for utility security profiles from outside of library SYSSEC.

NSCUT is invoked as follows:

```
CALLNAT 'NSCUT' PFUNCTION PUTILITY PUSER PLIBRARY PRC PPFKEY(*)
          PPARM PPARM1 PPARM2 PTEXT(*) PNC-MESSAGE
```

Example programs PGMUT_{nnn} of how to invoke subprogram NSCUT, as well as explanatory texts TXTUT_{nnn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMUT_{nnn} and TXTUT_{nnn}.

The first parameter (PFUNCTION) has to be filled with the function code for the desired function. The following functions are available:

Code	Subfunction
AD	Add utility
DE	Delete utility
DI	Display utility
MO	Modify utility (including all components of its security profile)

Please note that the components of the security profiles are different for each utility; see also the sources of PGMUT_{nnn}.

Subprogram NSCXLO

The subprogram NSCXLO is used to read maintenance log records, which are created by Natural Security if the general option “Logging of Maintenance Functions” is active.

NSCXLO is invoked as follows:

```
CALLNAT 'NSCXLO' PFUNCTION PSELECT-TYPE PSTART-OBJ-ID  
                PFROMTIMESTAMP PTOTIMESTAMP PRC PPARAM PPARAM1(*) PNSC-MESSAGE
```

Example programs PGMXLO_{nn} of how to invoke subprogram NSCXLO, as well as explanatory texts TXTXLO_{nn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMXLO_{nn} and TX-TXLO_{nn}.

Subprogram NSCXR

The subprogram NSCXR is used to perform cross-reference functions for security profiles from outside of library SYSSEC.

NSCXR is invoked as follows:

```
CALLNAT 'NSCXR' POBJ-TYPE POBJ-ID PLINK-ID PRC SUB-TYPE  
                PPARAM PPARAM2(*) PNSC-MESSAGE
```

Example programs PGMXR_{nnn} of how to invoke subprogram NSCXR, as well as explanatory texts TXTXR_{nnn}, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMXR_{nnn} and TXTXR_{nnn}.

The first parameter (POBJ-TYPE) has to be filled with the code for the type of object for which a function is to be performed:

Code	Object Type
US	User
LI	Library
DD	DDM (this object type is not available on mainframes)
FI	File (this object type is only available on mainframes)
MA	Mailbox
LE	Logon error record
LR	Logon record

Code	Object Type
ST	Steplib
UT	Utility
CP	Command processor
PE	Predict external object (this object type is only available if Predict is installed)
PF	Predict function (this object type is only available if Predict is installed)
PL	Predict 3GL library (this object type is only available if Predict is installed)
PO	Predict documentation object (this object type is only available if Predict is installed)
SF	System file

For the individual object types listed above, the following functions can be performed by filling the parameter SUB-TYPE with one of the following function codes:

Function Available for Every Object Type:

Code	Function
TR	Translates the 2-character object-type code into the corresponding object type.

Functions Available for a User (US):

Code	Function
*	List all users.
A	List all users of type ADMINISTRATOR.
P	List all users of type PERSON.
M	List all users of type MEMBER.
T	List all users of type TERMINAL.
G	List all users of type GROUP.
B	List all users of type BATCH.
GR	List all groups the user belongs to.
GP	List all privileged groups the user belongs to.
GM	List all users contained in the group.
BU	List all users in whose security profiles the batch user ID is specified.
NI	Retrieve the user ID belonging to a specified user name.
LA	List all libraries available to the user.
LL	List all libraries to which the user is linked.
LD	List all libraries to which the user is linked directly.
LG	List all libraries to which the user is linked by means of a group.
LP	List all libraries to which the user is linked by means of a privileged group.
OW	List all security profiles owned by the user.

Code	Function
DD	List all DDMs available to the user (this function is not available on mainframes).
DL	List all DDMs available to the user by means of a special link (this function is not available on mainframes).
FI	List all files to which the user's private library is linked (this function is only available on mainframes).
UT	List all utility profiles which apply to the user.

Functions Available for a Library (LI):

Code	Function
*	List all libraries and users' private libraries.
L	List all libraries.
U	List all users' private libraries.
NI	Retrieve the library ID belonging to a specified library name.
DD	List all DDMs to which the library is linked (this function is not available on mainframes).
LD	List all DDMs to which the library is linked by means of a special link (this function is not available on mainframes).
FI	List all files to which the library is linked (this function is only available on mainframes).
NO	List allowed/disallowed modules.
SM	Retrieve information on users' access rights to a single module in the library.
US	List all users linked to the library.
UT	List all utility profiles which apply to the library.
CP	List all command processors for the library that have a specific status.

Functions Available for a DDM (DD):

Code	Function
*	List all defined DDMs (that is, for which security profiles exist).
UN	List all undefined DDMs (that is, for which no security profiles exist).
DD	List all defined and undefined DDMs.
P	List all DDMs with external status PUBLIC.
A	List all DDMs with external status ACCESS.
U	List all DDMs with external status PRIVATE.
ND	List all DDM security profiles for which no corresponding DDMs exist.
LI	List all libraries which are linked to the DDM.
US	List all users which are linked to the DDM.
SL	List all DDM definitions in special link security profiles.
X	List all DDM definitions in library and special link security profiles.

Functions Available for a File (FI):

Code	Function
PU	List files of type PUBLIC.
AC	List files of type ACCESS.
UP	List files of type PRIVATE.
DD	List files with existing DDM.
ND	List files with no DDM.
UN	List undefined files.
LI	List libraries to which the specified file is linked.
US	List users whose private libraries are linked to the specified file.

Functions Available for a Mailbox (MA):

Code	Function
LI	List all libraries to which the mailbox is assigned.
US	List all users to which the mailbox is assigned.

Functions Available for Logon Error Records (LE):

Code	Function
P	List logon error records, in order of TP user IDs.
T	List logon error records, in order of terminal IDs.

Functions Available for Logon Records (LR):

Code	Function
L	List logon records, in order of library IDs.
U	List logon records, in order of user IDs.
LX	List logon records to undefined libraries (in order of library IDs).
UX	List logon records of undefined users (in order of user IDs).

Functions Available for Steplibs (ST):

Code	Function
*	List all steplibs.
LK	List protected steplibs.
NN	List public steplibs.
SL	List special linked steplibs.

Functions Available for Utilities (UT):

Code	Function
LI	List all library-specific utility profiles defined for the utility.
US	List all user-specific utility profiles defined for the utility.
UT	List all utility profiles defined for the utility.
<i>blank</i>	List all utility profiles defined for all utilities.

Functions Available for Command Processors (CP):

For a command processor, NSCXR will list all libraries and users for the command processor (without any SUB-TYPE specification being required).

Functions Available for Predict Objects (PE, PF, PL, PO):

For each of the four Predict object types, NSCXR will list all objects of that type (without any SUB-TYPE specification being required).

Functions Available for System Files (SF):

Code	Function
FN	List all libraries of the current FNAT system file which are not defined in Natural Security.
FU	List all libraries of the current FUSER system file which are not defined in Natural Security.

Function Available for External Objects:

Code	Function
LU	List all users who are linked to the external object.

Subprogram NSCXRIER

The subprogram NSCXRIER is used to display individual logon error records (similar to the Logon/Countersign Errors function “Display individual error entries”).

NSCXRIER is invoked as follows:

```
CALLNAT 'NSCXRIER' NSCXRIER-PARM PNSC-MESSAGE
```

An example program PGMXRIER of how to invoke subprogram NSCXRIER, as well as an explanatory text TXTXRIER, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMXRIER and TXTXRIER.

Subprogram NSCXRUSE

The subprogram NSCXRUSE is used in conjunction with the **Lock User Option** set to “X” to obtain a list of users whose logon error counters are greater than “0”.

It is also used in conjunction with the general option **“Record Each User's Logon Daily”**. When this option is active, NSCXRUSE can be used to display the IDs of users who have not logged on to Natural since a specified date.

NSCXRUSE is invoked as follows:

```
CALLNAT 'NSCXRUSE' POBJ-TYPE POBJ-ID PRC PSUBTYPE PPARAM PPARAM2(*) PNSC-MESSAGE
```

An example program PGMXRUSE of how to invoke subprogram NSCXRUSE, as well as an explanatory text TXTXRUSE, are provided in source form in the library SYSSEC.

The individual CALLNAT parameters are explained in the source codes of PGMXRUSE and TXXRUSE.

See also the subprogram **NSC---SP**.

Subprogram SECNOTE

The subprogram SECNOTE is used to display the Security Notes part of a security profile. It can be applied to a user, group, library or special link security profile.

The object module of SECNOTE is stored in the library SYSTEM. The source code of SECNOTE is not available.

SECNOTE has to be invoked with the following parameters:

Parameter	Explanation	
#TYPE (A1)	With this parameter, you specify the type of object whose Security Notes are to be read. Valid values for #TYPE are:	
	U	User. The current content of the Natural system variable *USER determines which user's Security Notes will be read.
	L	Library. The current content of the Natural system variable *APPLIC-ID determines which library's Security Notes will be read.
	G	Group. The current content of the Natural system variable *GROUP determines which user's/group's Security Notes will be read.
	S	Special Link. The current contents of the Natural system variables *GROUP and *APPLIC-ID determine which special link's Security Notes will be read.
#NOTES (A60/8)	On return from SECNOTE, this parameter contains the Security Notes.	
#RC (N4)	This parameter contains the return code from SECNOTE. Possible return codes are:	
	0	Security Notes have been read.
	860	#TYPE contains invalid code.
	806	Library does not exist (is not defined to Natural Security).
	861	User has no special link to library.
	873	User does not exist (is not defined to Natural Security).

The above-mentioned system variables are described in the Natural *System Variables* documentation.

26

Add-On Products and Plug-Ins

■ Plug-Ins under Natural Security	396
■ SYSDIC under Natural Security	397
■ SYSAOS under Natural Security	398

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

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.

Index

N

Natural Security, 1

