Protecting the Natural Development Server Environment and Applications

Protecting the Natural Development Server Environment and Applications

This section covers the following topics:

- Protecting the Natural Development Server Environment
- Protecting Natural Development Server Applications

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	*Client action not validated by the server*.

Location in Tree View	Action	Controlled by
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.
	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.

Location in Tree View	Action	Controlled by
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	*Client action not validated by the server.*	-
Copy	Co	Copy
Move	Mo	Cut and Paste
Delete	De	Delete
Rename	Ren	-
Import	*Client action not validated by the server.*	-

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, CATALL, 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 a "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 ist 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 -------                            Library  DBID  FNR  NSC
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. **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)	The IDs of the libraries which are linked to the application in the Natural Development Server. 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. 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.)
DBID / FNR (display only)	For each library, the database ID and file number of its FUSER system file are displayed.

Field	Explanation
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 -------              Base Application                NSC
Y R Read                                   ABCB0012-BASE-APPL               X
* A Add                                    ABCB0015-BASE-APPL
Y M Modify                                 ABCB0019A01                      X
N D Delete









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.

Field	Explanation	
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)	The following information is displayed: • 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	You may enter up to eight IDs of ADMINISTRATORs. Only the ADMINISTRATORs specified here will be allowed to maintain the security profile. If no owner is specified, any user of type ADMINISTRATOR may maintain the security profile. 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. For an explanation of owners and co-owners, see the section *Countersignatures*.

Invoking Application Maintenance

Application maintenance can only be invoked if the prerequisites described above are met.

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

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

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

Selecting an Application for Processing

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

If you do not wish to get a list of all existing application profiles, but would like only certain applications 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 "Application" with a character or with the cursor (and, if desired, enter a start value and/or application type). The Application Maintenance selection list will be displayed:

```
14:49:01                    *** NATURAL SECURITY ***                 2009-07-31
                          - Application Maintenance -

 Co Application                          Type Status Access  Message
 __ _____________________________________ ____  ____ ________ ________________________
 __ * Base Application *                 Base  NApp RAM
 __ A                                    Base  Defi * *D
 __ ABC                                  Base  Defi ** *
 __ ABCB0014-BASE-APPL                   Base  Defi RAMD
 __ ABCB0015-BASE-APPL                   Base  NApp RA
 __ ABCB0016-BASE-APPL                   Base  Defi RAMD
 __ ABCB0017-BASE-APPL                   Base  NApp RAM
 __ ABCXYZ                               Base  Defi * *
 __ ABCXYZ1                              Base  Defi RA
 __ ABCXYZ2                              Base  Defi R***
 __ * Compound Application *             Comp  NApp R
 __ COMP                                 Comp  Defi RAMD
 __ COMP-APPLIC                          Comp  Defi R**
 __ COMP-APPLIC-DEP                      Comp  Defi RAM*


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

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):

blank	All application security profiles - regardless of whether or not a corresponding application exists.
A̲LL	All applications - regardless of whether or or not a corresponding security profile has been defined.
D̲EFI	Defined; that is, applications for which security profiles have been defined.
U̲NDF	Undefined; that is, applications for which no security profiles have been defined.
N̲APP	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
AD	Add application
CO	Copy application
MO	Modify application
RE	Rename application
DE	Delete application
DI	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

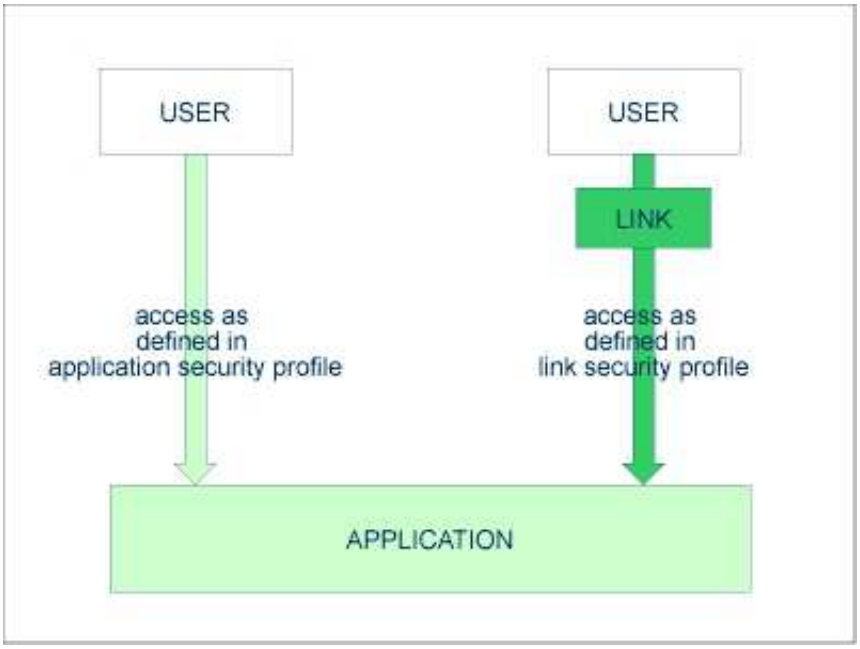
The Display Application function is used to display an existing application security profile.

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.
DI	Display Application - The application security profile will be displayed.
DL	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.
DI	Display User - The user security profile will be displayed.
DL	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.