Structure And Terminology Of Natural Security

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

- Users
- Libraries
- Links Between Users and Libraries
- DDMs/Files
- Utilities
- Applications
- RPC Servers
- Other Object Types
- Profile Parameters

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:

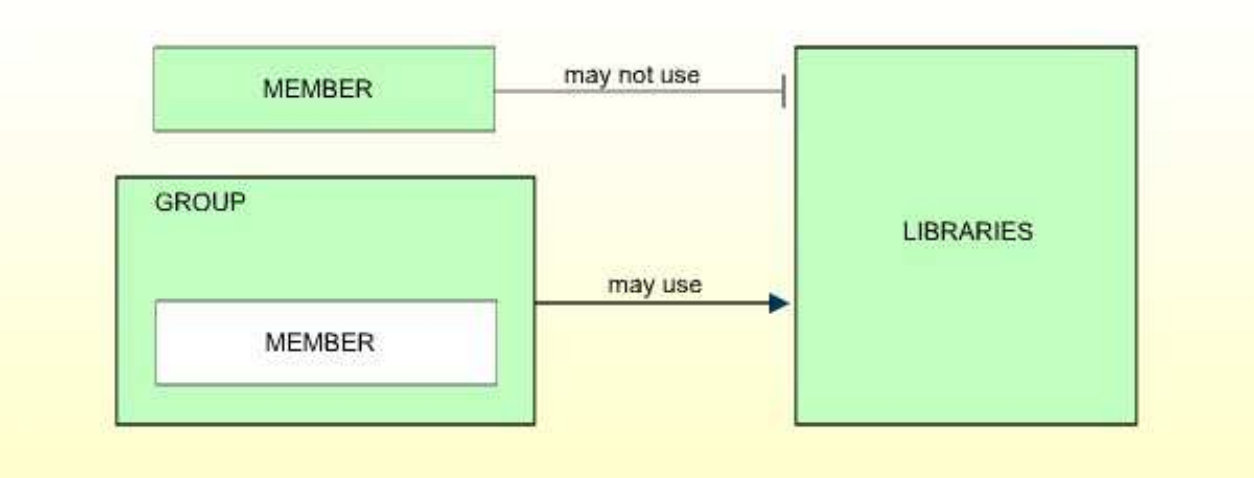
- GROUP

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

- BATCH

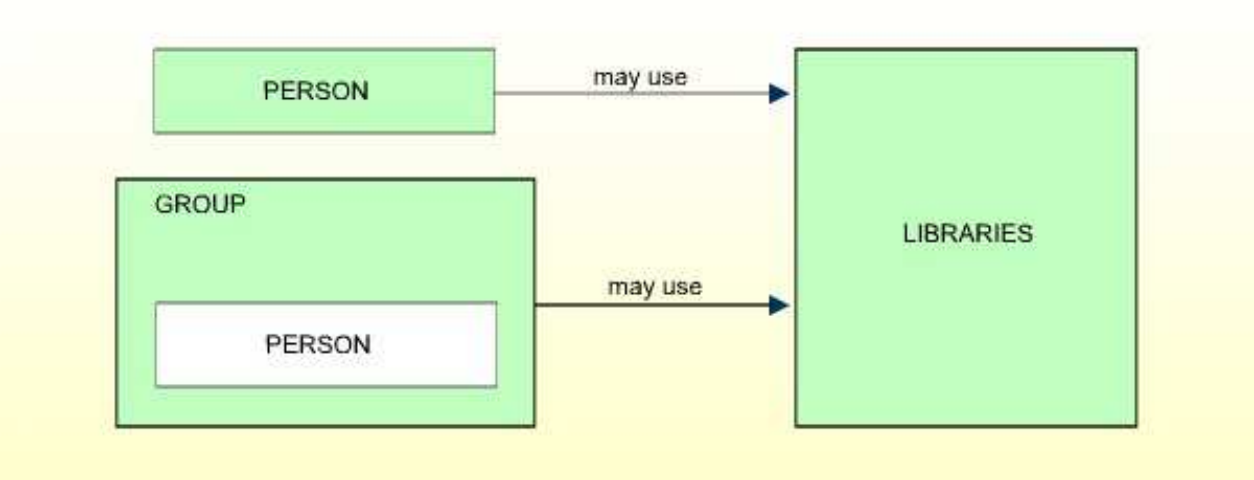
User Type MEMBER

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.

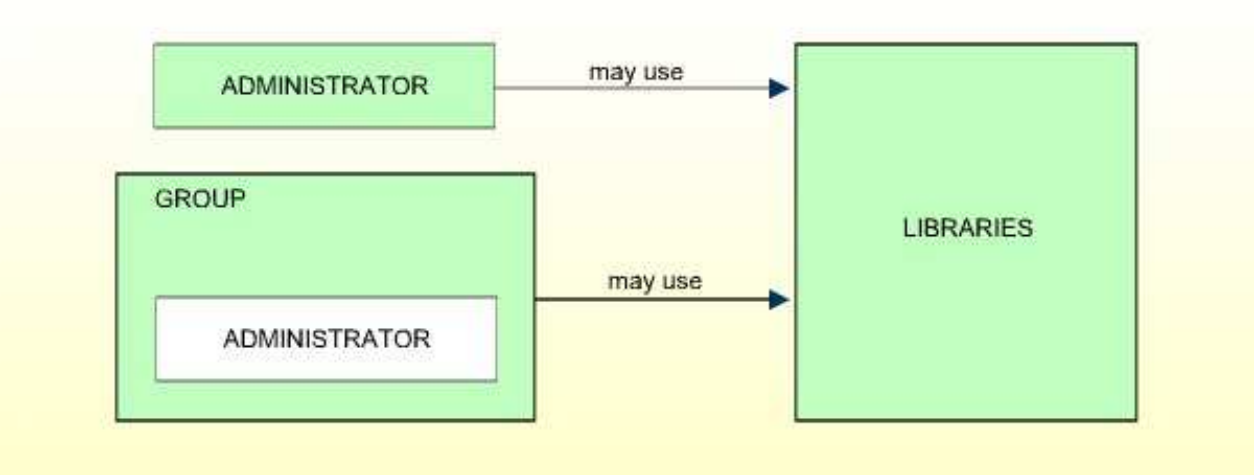


User Type ADMINISTRATOR

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.

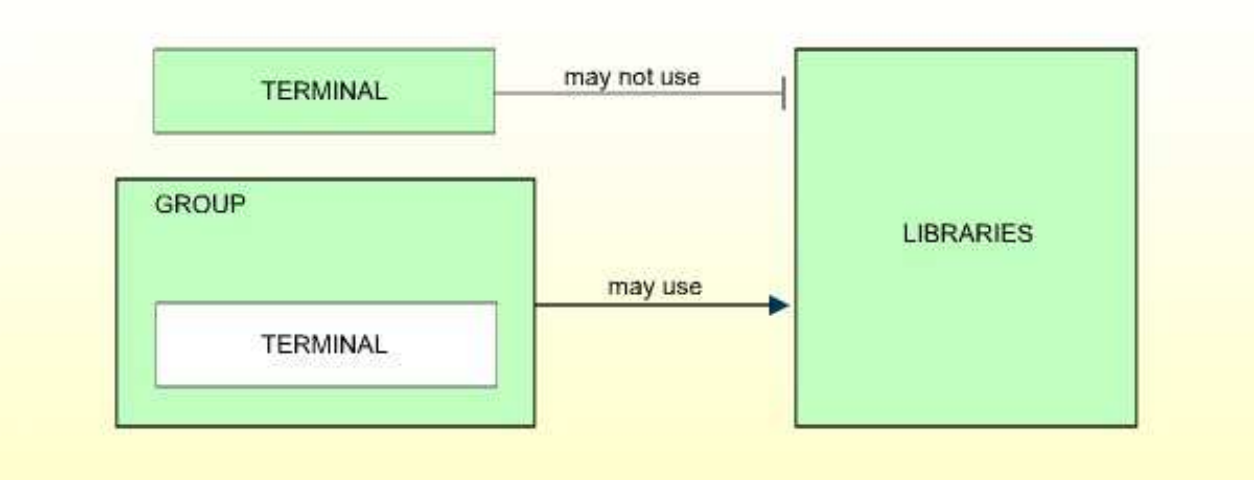
This user type is only for those users who are to be system administrators of Natural Security.



User Type TERMINAL

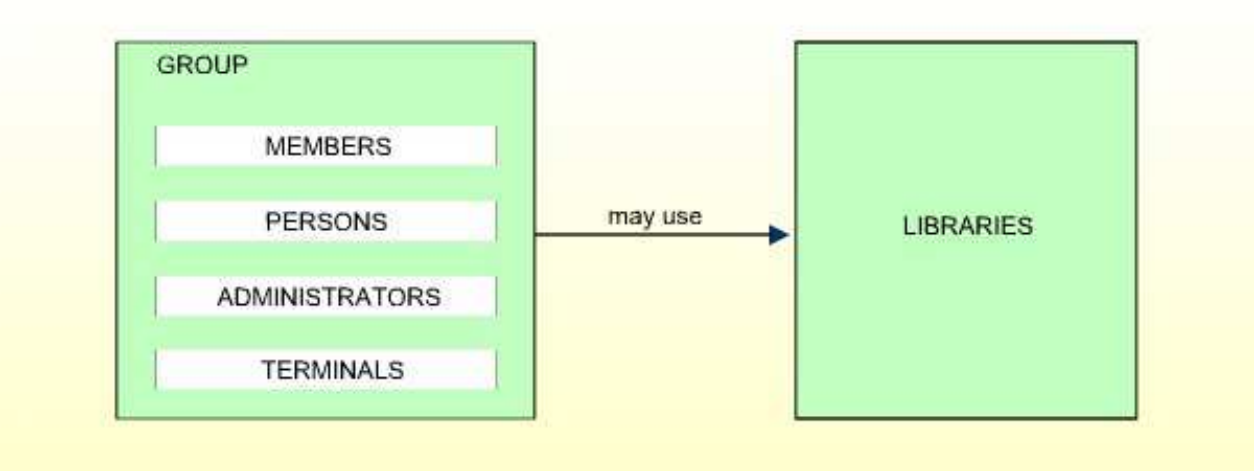
This user type applies to terminals only. Terminals do not necessarily have to be defined. The definition of terminals becomes relevant only in connection with libraries which are to be used from certain terminals only.

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.

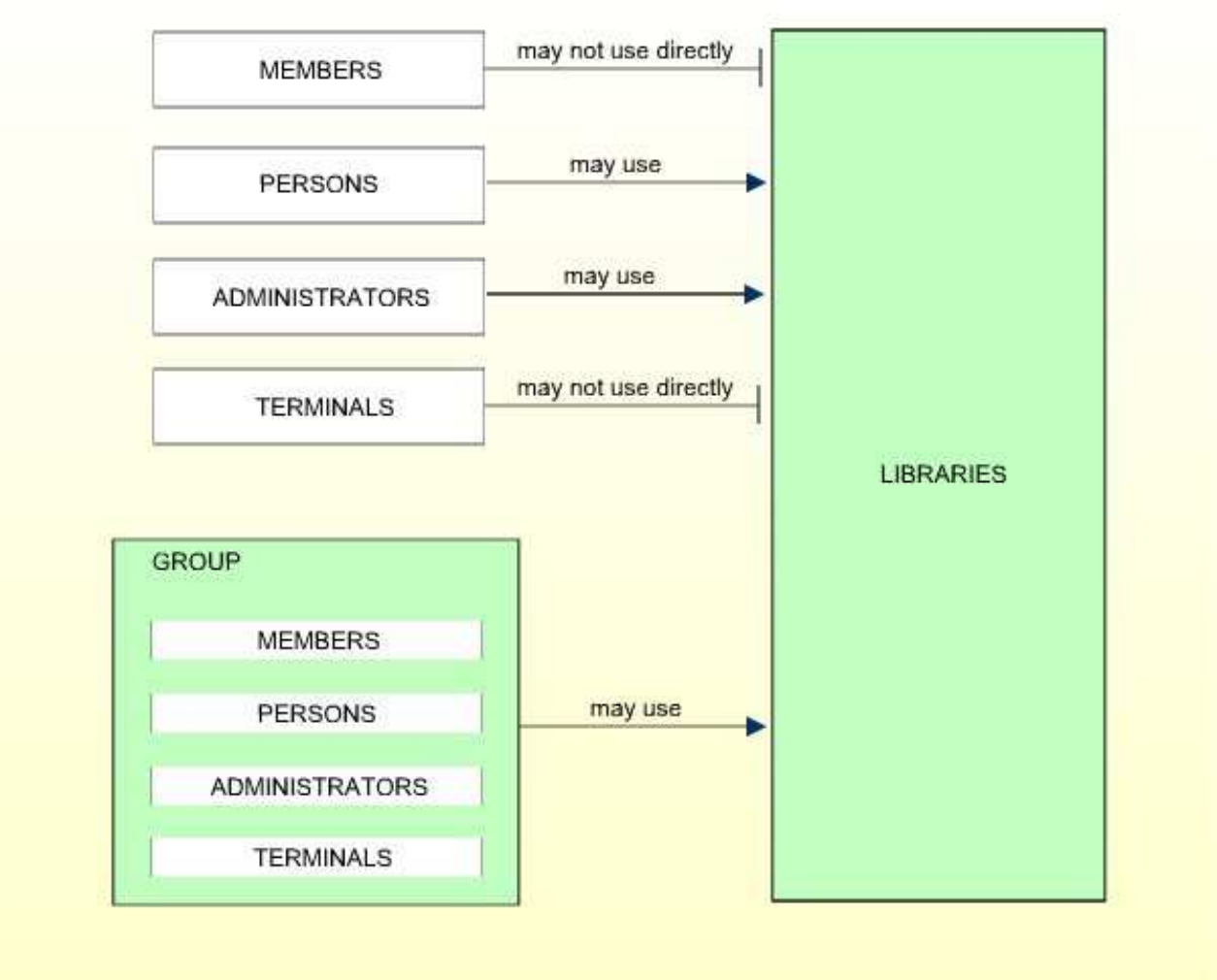
It cannot be compared directly with the other user types, and is only mentioned here for the sake of completeness. For details on this user type, see *Batch User Security Profiles* in the section *Natural Security In Batch Mode*.

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

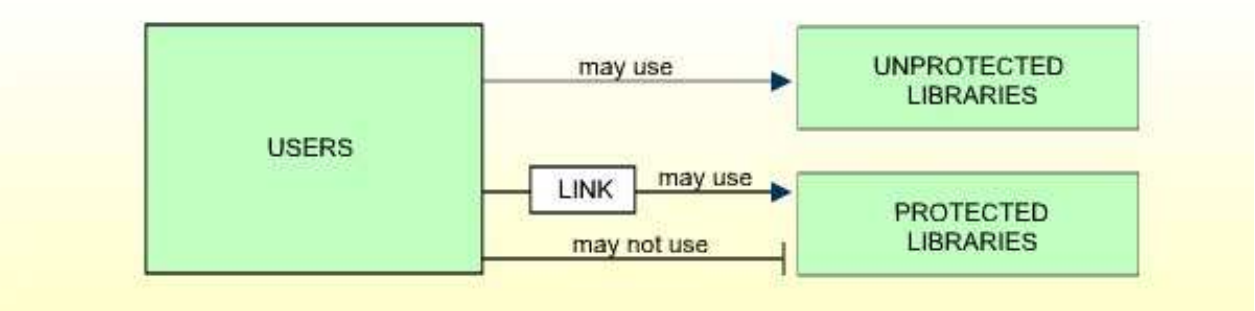
These may be used by any user without a special relationship having to be defined. (Remember that only users of type ADMINISTRATOR or PERSON may use libraries directly. MEMBERS and TERMINALS may use libraries only through membership in a GROUP.)

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 *linked* to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been *linked* 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 *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 *linked* to it.
PRIVATE	The DDM is protected. It can be used only by libraries which have been *linked* to it. This *link* 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.

Profile Parameter	Corresponding Setting in Natural Security
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.
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.