User Maintenance

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

- Before You Begin
- Components of a User Profile
- Creating and Maintaining User Profiles

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:

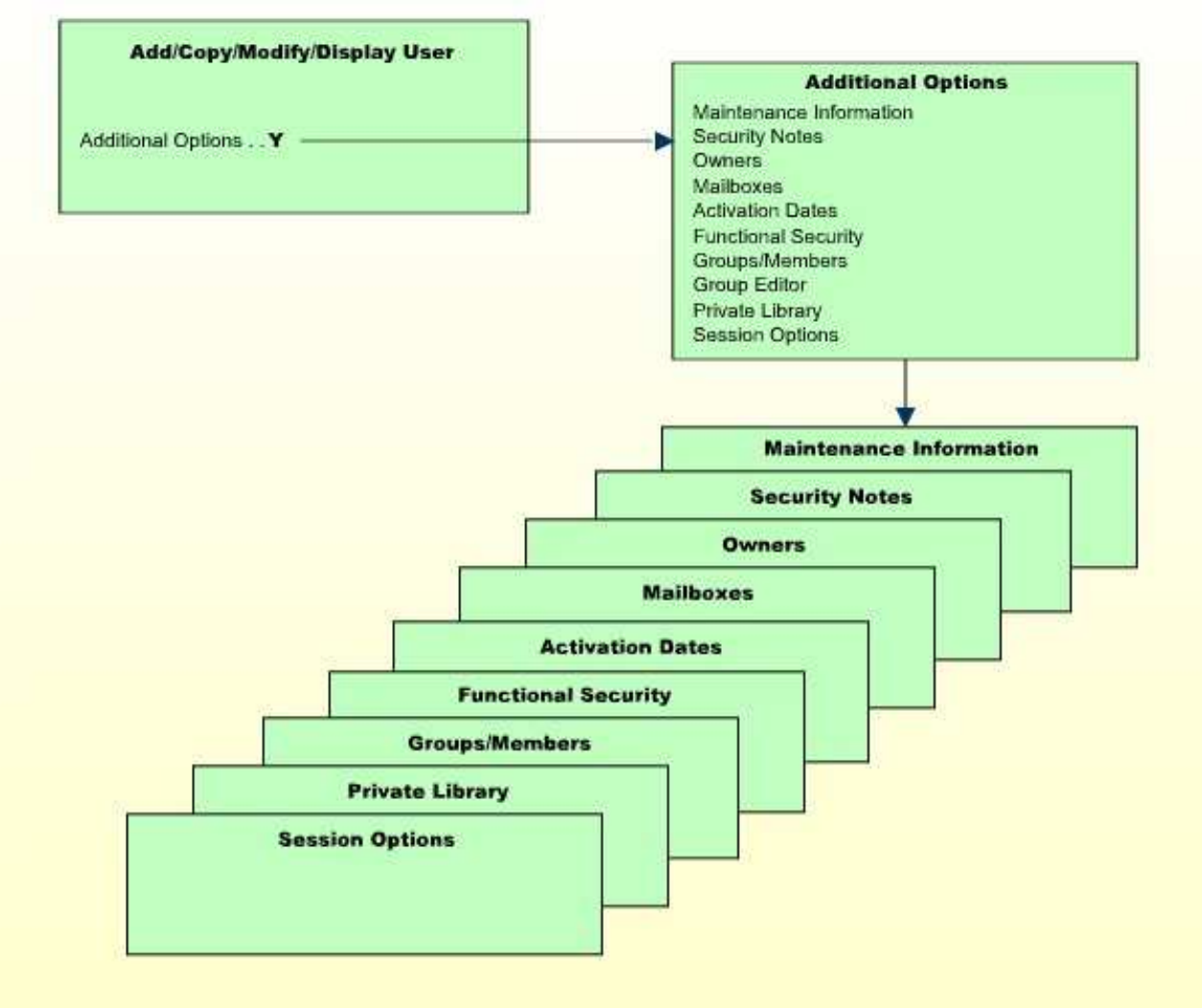
1. Create a group security profile; that is, define a user of type GROUP.
2. Create individual user security profiles; that is, define users (typically of type MEMBER).
3. Assign MEMBERs to the GROUP; that is, modify the GROUP security profile.

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 ***                 2008-01-18
                                - Modify User -

                                                 Modified ..          by
 User ID ...... AD
 User Name .... ARTHUR DENT_____________________
 User Type .... A (A=Administrator, P=Person, M=Member)

 Privil. Groups          Libraries               Password
 --------------      -------------------      ----------------------
    DOC_____         Default .. SYSSEC__      New Password ________
    ________         Last .....               Change after 666 days
    ________
    ________               ETID               Batch User ID ..... ________
    ________         -------------------      Language .......... 0
                     Default ..  AR1R  G      Private Library ... N
 No. groups   3      Last .....               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, T = Terminal B = Batch User

Field	Explanation
Privileged Groups (A, P, M, T, B)	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: • 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. 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 *Protecting Utilities* for details. You may enter a group in the Privileged Groups list only after the user has been added to the group. If you remove a group from the user's Privileged Groups list, the user will *not* be deleted as a member of that group.
Members (G)	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). You can assign users to a group only after they have been defined to Natural Security.
No. of Groups (A, P, M, T, B; display only)	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.

Field	Explanation
No. of Members (G; display only)	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.
Default Library	In this field, you may enter the ID of a default library. • 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. • 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.)

Field	Explanation
Default ETID (A, P, M, T, B)	This field displays the ID to identify End of Transaction data (ETID). ● 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 *Administrator Services* 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*. **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.
Last ETID (A, P, M, T, B; display only)	The ETID which was last generated/set for the user.
New Password (A, P, M)	You may enter a password for the user to be used when he or she logs on. 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). If no password is entered here, Natural Security will assume the password to be identical to the user ID. The minimum length of the password is set in the *Library and User Preset Values* section of Administrator Services.
Change after *nnn* days (A, P, M)	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. 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. 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 logon.

Field	Explanation
Batch User ID (A, P, M, G)	If the Natural system variable *DEVICE is set to "BATCH", the following applies: 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. 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. **Note:** This option only applies if the Natural system variable *DEVICE is set to "BATCH"; otherwise, this option has no effect.
Language (A, P, M, G, B)	This corresponds to the Natural system variable *LANGUAGE and controls the usage of Natural error messages. 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. For further information, see the system variable *LANGUAGE and the profile parameter ULANG (in the Natural *System Variables* and *Parameter Reference* documentation respectively).

Field	Explanation
Time Differential (T, G)	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 Natural *Parameter Reference* documentation). 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). 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. 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 be comparison of physical and logical machine times). You can use either Time Differential or Time Zone (described below), but not both.
Time Zone (T, G)	This only applies to an environment in which remote nodes are used in a computer network. 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 NATCONFG. The definition in the NTTZ macro determines the number of hours/minutes added to/subtracted from computer centre time to obtain local time. You can use either Time Zone or Time Differential (described above), but not both.
Private Library (A, P)	This option determines whether the user may have a private library (see below).
Logon recorded	All logons by the user to any library will be recorded. See Logon Records in the section *Administrator Services* for information on logon records.

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)	In this window, 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	In this window, you may enter your notes on the security profile.

Additional Option	Explanation
Owners	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. 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 information on owners and co-owners, see the section *Countersignatures*.
Mailboxes	In this window, you may enter up to five mailbox IDs. For information on mailboxes, see the section *Mailboxes*.
Activation Dates (A, P, M, G)	In this window, you may define dates as of which or until when the security profile shall be valid. 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.
Functional Security	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. This is only relevant if command processors have been created with the Natural utility SYSNCP. See the section *Functional Security* for details.
Groups/Members (display only)	If you mark this field, a list of all groups to which the user belongs will be displayed. If the user is a GROUP, a list of all users who belong to the GROUP will be displayed.
Group Editor (G)	If you mark this field, the Edit Group Members function will be invoked. This function is explained under *Editing Group Members* below.

Additional Option	Explanation
Private Library (A, P)	A user may have a "personal" library whose ID is the same as his/her user ID. Such a library is called a *private library*. Private libraries can be made available in two modes: • **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 *Protecting Libraries*). • **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 *not* be used. The mode is set with the general option "Private libraries in public mode" (described in the section *Administrator Services*) and applies to all private libraries. For information on creating and maintaining a private library, see the section *Library Maintenance*. As far as access to DDMs/files is concerned, there is no difference between private libraries and "normal" libraries. **Note:** Unless explicitly stated otherwise, what is said in the Natural Security documentation about libraries also applies to private libraries.
Session Options (A, P, G)	See below.

Session Options

Option	Explanation
Unlock Objects	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: **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. The default value is "Y".
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 *Protecting Environments*.
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.

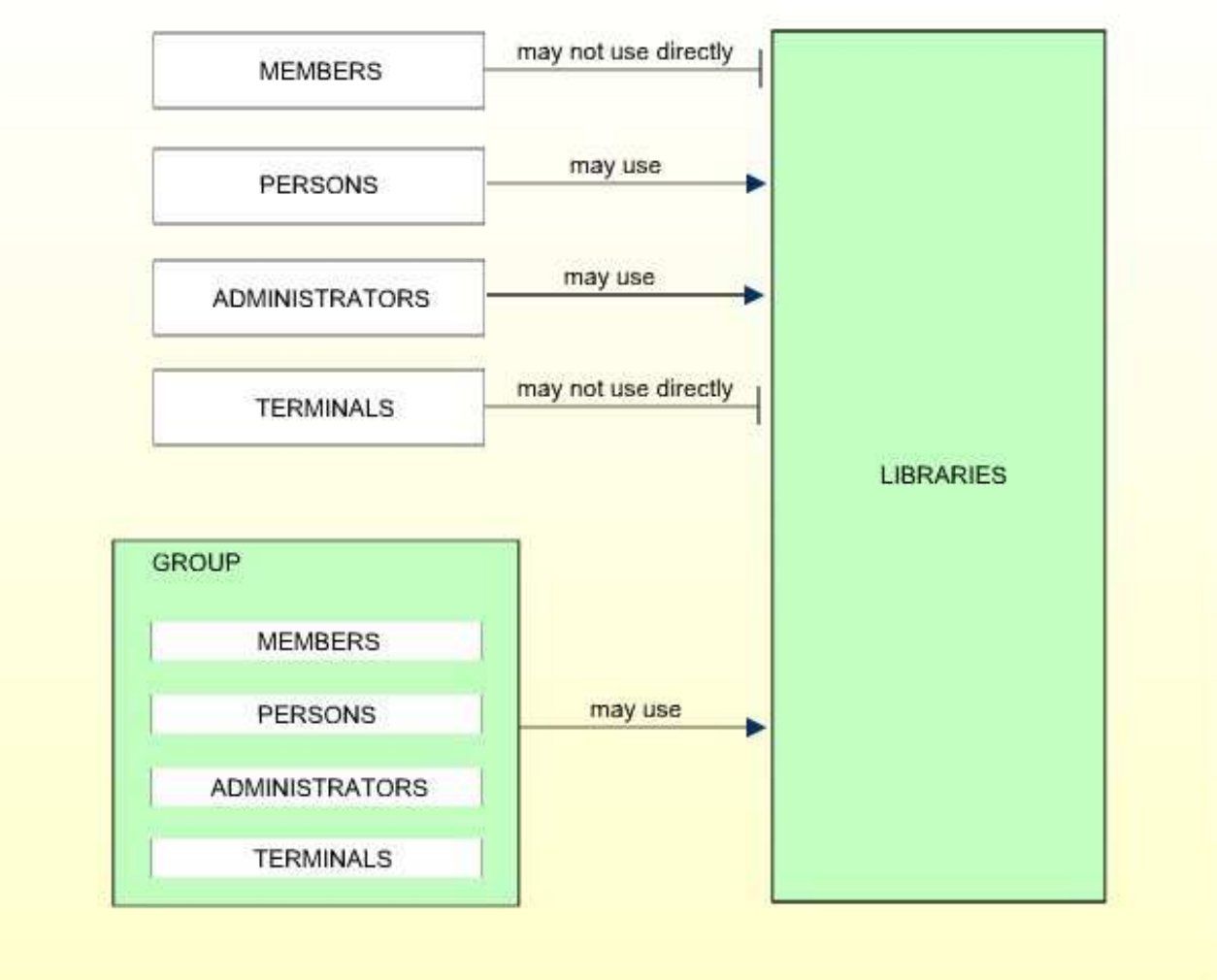
User Type

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 *Natural Security In Batch Mode*)

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 ***                  2008-10-31
                              - 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---
       Help        Exit              Flip  -     +                       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**
CO	Copy user
MO	Modify user
RE	Rename user
DE	Delete user
DI	Display user
EG	Edit group members
LA	Link user to applications
LL	Link user to libraries
LO	Link user to external objects
CP	Copy user’s links
EP	Protect environments for user
MD	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 *not* 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.