Administrator Services

This section covers the following topics:

- Access to Administrator Services
- General Options
- PF-Keys
- Logon/Countersign Errors
- Logon Records
- Maintenance Log Records
- SAF Online Services
- User Default Profiles
- Library Default Profiles
- Library and User Preset Values
- Definition of System Libraries
- Definition of Undefined Libraries

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

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

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

Administrator Services Menu 1:

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

Administrator Services Menu 2:

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

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

Access to Administrator Services

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

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

For information on owners in library security profiles, see the sections *Library Maintenance* and *Countersignatures*.

General Options

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

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

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

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

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

General Options - Screen 1:

- Transition Period Logon
- Activate Security for Development Server File
- Maximum Number of Logon Attempts
- Suppress Display of Logon Messages
- Lock User Option
- User Password History
- Free Access to Functions via APIs
- Minimum Number of Co-Owners
- Deletion of Non-Empty Libraries Allowed
- Overwriting of Defaults Possible
- Display DBID/FNR of FSEC
- Exit Functions with Confirmation
- Logging of Maintenance Functions

General Options - Screen 2:

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

The individual options are described below.

Transition Period Logon

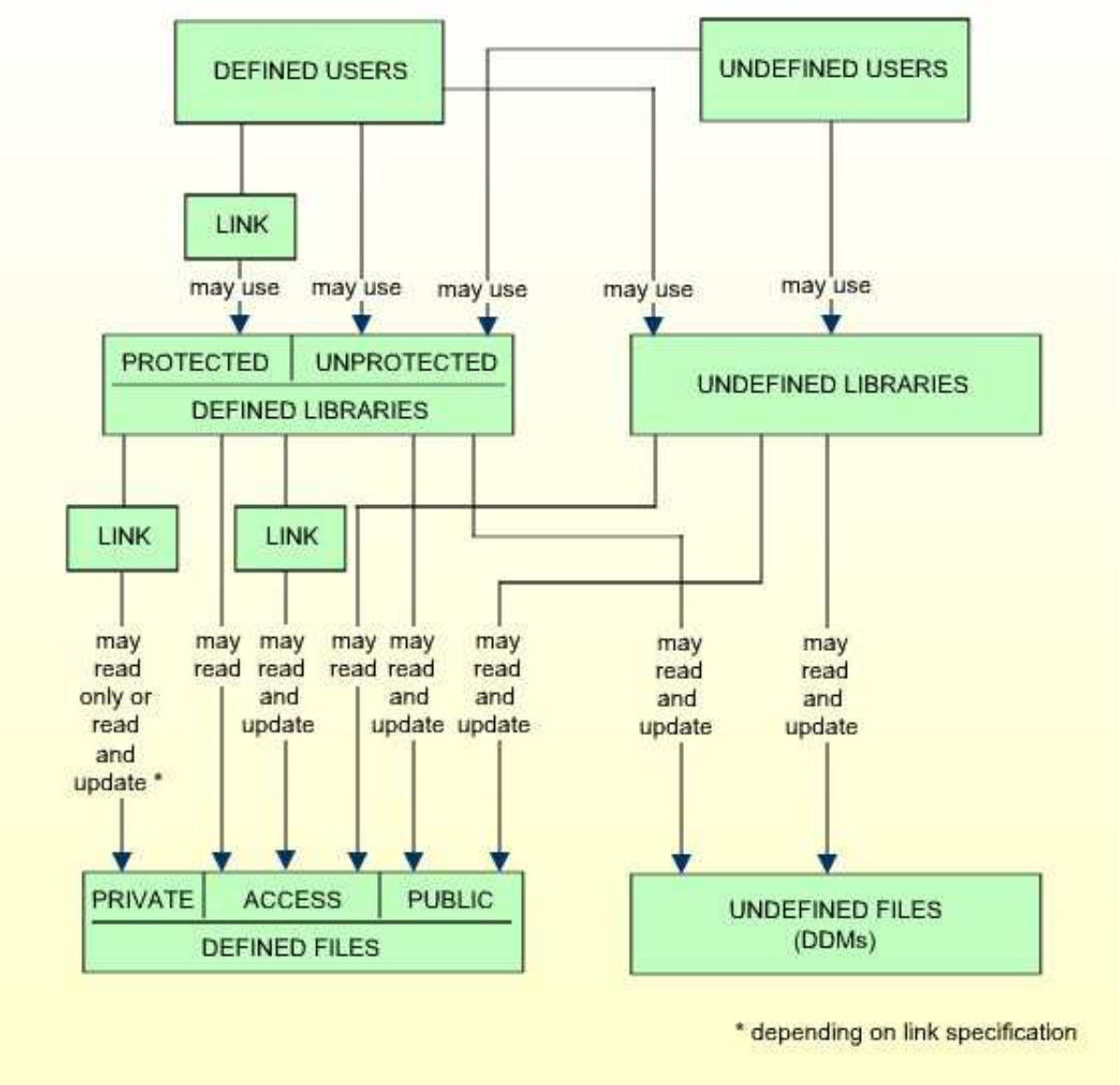
This option allows a smooth transition from an unprotected Natural environment to one protected by Natural Security.

Y	• Users not yet defined to Natural Security may log on to libraries which are not yet defined to Natural Security or which are defined as unprotected. • Libraries not yet defined to Natural Security may be accessed by any (defined or undefined) user. • Undefined libraries may access DDMs which are not yet defined to Natural Security as well as files of status PUBLIC and ACCESS. • Undefined DDMs may be accessed by any (defined or undefined) library.
N	Only users defined to Natural Security may use Natural. Any library not defined to Natural Security cannot be used.

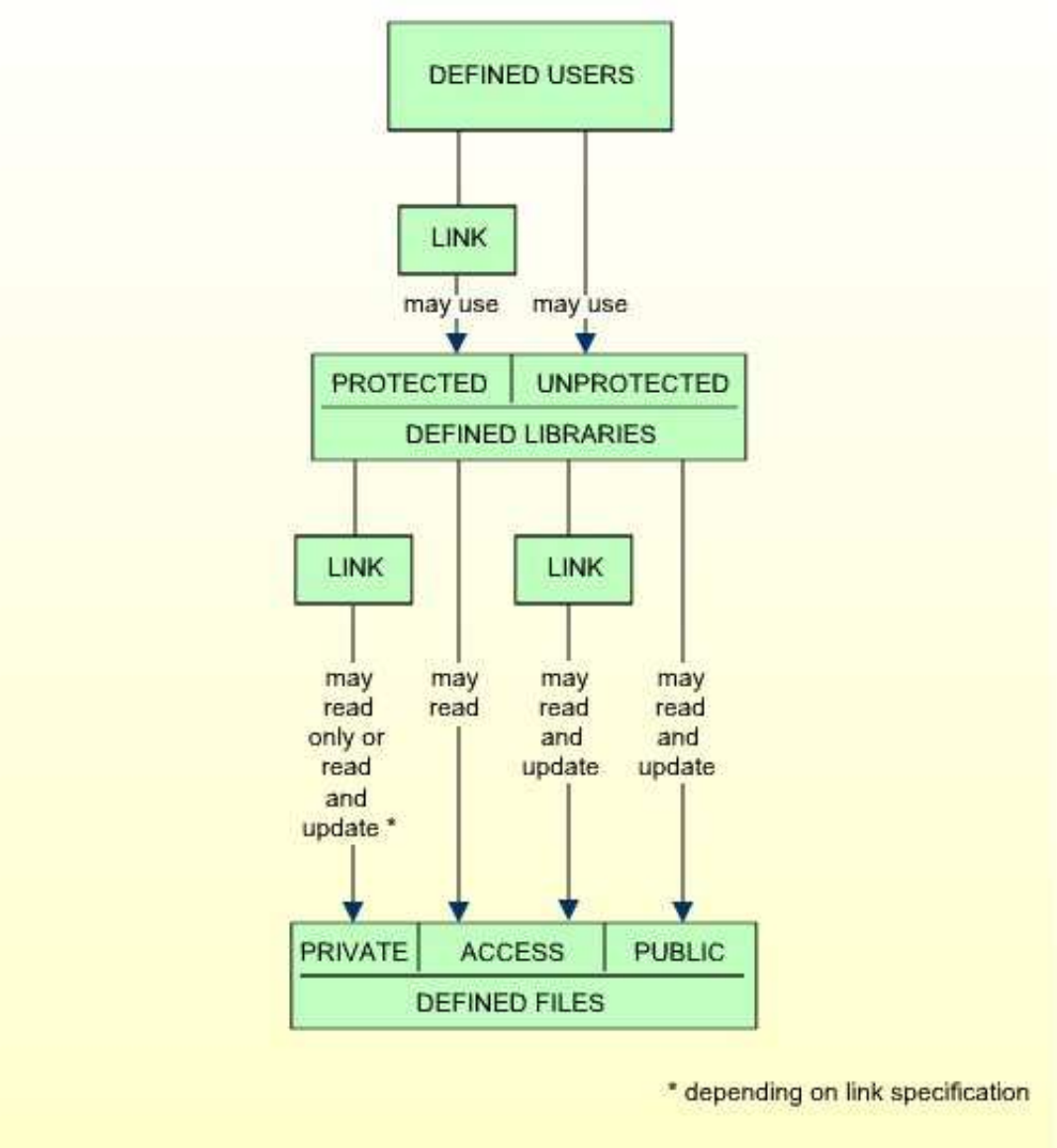
The effects of the Transition Period Logon settings are illustrated below.

If you have had an unprotected Natural installation and now have installed Natural Security for the first time, it is advisable to set the Transition Period Logon to "Y" so as to ensure that work with Natural may continue while users and libraries are defined to Natural Security. Once all objects and links are defined, the Transition Period Logon should be set to "N".

Conditions of use under Transition Period Logon = Y:



Conditions of use under Transition Period Logon = N:



Activate Security for Development Server File

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

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

Maximum Number of Logon Attempts

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

Suppress Display of Logon Messages

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

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

Lock User Option

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

Y	**Logon:** For logon attempts, the following applies: Once a user has reached the maximum number of logon attempts without entering the correct password, the respective user will be locked, that is, the user ID will be made "invalid". The following will be locked: • all Natural Security user IDs which were tried out, • the user's operating-system login name (as identified by the Natural system variable *INIT-USER), if a Natural Security user profile exists whose ID corresponds to that name. **Countersignatures:** For countersign attempts, the following applies: After too many invalid passwords (the maximum number of logon attempts also applies here) on a Countersign screen, the user who invoked the respective function (as identified by his/her Natural Security user ID) will be locked.
F	**Logon:** For logon attempts, "F" has the same effects as "Y" - in addition, the Natural session is terminated when the user is locked. **Countersignatures:** For countersign attempts, "F" has the same effect as "Y".
X	**Logon:** For logon attempts, "X" has the same effects as "F"- except that Natural Security "remembers" unsuccessful attempts across sessions: With "Y" and "F", the counters of logon attempts for the user IDs which were tried out unsuccessfully is reset when the user aborts the logon procedure. With "X", however, these error counters are kept for logon procedures in subsequent sessions, thus reducing the number of subsequent logon attempts with these user IDs. This means that the chances of someone gaining access with another user's ID are reduced considerably. With "X", the error counter for a user ID is only reset after a successful logon. **Countersignatures:** For countersign attempts, "X" has the same effect as "Y". A user's error counters can be displayed by pressing PF16 in his/her security profile. A list of all users whose error counters are greater than "0" can be obtained with the application programming interface NSCXRUSE.
N	The Lock User feature is not active.

Natural RPC Service Calls

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

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

User Password History

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

Y	Password history is active. This has the following effects: • The last *nn* passwords used by each user are recorded by Natural Security. These last *nn* passwords cannot be used again by the user as new password. You set the number of passwords to be recorded in the window displayed when you activate this option. Possible values: 1 - 99. • A user is forced to change his/her password at logon when the password has been changed by an administrator in the user's security profile. • You can define certain rules to which passwords must conform. You define these password rules by using the function "Library and User Preset Values" (see below).
N	Password history is not active.

Other password-related Natural Security features are:

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

Free Access to Functions via APIs

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

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

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

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

Minimum Number of Co-Owners

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

For an explanation of co-owners, see the section *Countersignatures*; leave the value set to "0" until you have read that section.

Deletion of Non-Empty Libraries Allowed

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

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

Overwriting of Defaults Possible

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

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

The preset values are described under *Library and User Preset Values* below.

Display DBID/FNR of FSEC

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

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

Exit Functions with Confirmation

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

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

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

Logging of Maintenance Functions

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

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

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

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

Log file DBID/FNR	The database ID and file number of the file in which the log records are to be stored. This file must have been loaded during the installation process of Natural Security.
	
	Note:
	Once "Logging of Maintenance Functions" has been activated, you cannot change the log file assignment. You have to deactivate the option, before you can assign another database ID or file number.
	
	Should the log file become inaccessible, and prevent you from deactivating the logging of maintenance functions, you can use the Natural system command INPL with code "R" (Recover) and option "A" (Adjust) to change the log file assignment. As parameters for the command you specify the database ID and file number of the current (inaccessible) log file and of its desired new location. Batch-mode input for this operation would be as follows:
	
	`//CMSYNIN DD *`
	`R,A`
	`old-DBID,old-FNR`
	`new-DBID,new-FNR`
	`.`

Logging even if no actual modification	Y - Modifications are also logged if nothing has actually been changed; that is, if a security profile or administrator services setting has been invoked for modification, but no actual change has been made to the profile/setting. N - Modifications are only logged if a profile/setting has actually been changed.

Logging of changes to	Possible values: N, Y, and (for user and library profiles) X. You mark with "Y" the object types whose modifications are to be logged: ● administrator services settings (*), ● user security profiles, ● library security profiles (including special link profiles), ● file security profiles, ● application security profiles, ● mailbox security profiles, ● various types of external object security profiles. (*) " Administrator services settings" in this context means all functions listed on the Administrator Services Menu (except "Application Programming Interfaces"). **Utility Profiles** Modifications to utility security profiles are not logged separately. Instead, default profiles and templates are handled under "administrator services settings", library-specific utility profiles under "library security profiles", and user-specific and user-library specific utility profiles under "user security profiles". **Extended Logging for User and Library Profiles** You can mark "user security profiles" and "library security profiles" with "X" (instead of "Y") for the following additional data to be logged. For user security profiles: ● When the Copy User function is used with the "with links" option, any relationship which the copying has established between the user and other objects is logged. ● When the Delete User function is used, any relationship which existed between the user and other objects and which was removed by the deletion is logged. For library security profiles: ● When the Copy Library function is used with the "with links" option, any relationship which the copying has established between the library and other objects is logged. ● When a link between a group and a library is maintained, a list of the group’s members is logged. ● When a maintenance functions affects the Disallow/Modules section of a library (or special link) profile, information on the changed status of any module is logged.

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

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

Concurrent Modifications Without Notification

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

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

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

Y	The modifications will be applied in any case.
N	A window will be displayed in which the administrator can choose to: • cancel his/her modifications, • apply his/her modifications, • return to the security profile in question.

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

Private Libraries in Public Mode

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

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

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

Suppress Mailboxes in Batch Mode

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

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

For information on mailboxes, see the section *Mailboxes*.

Environment Protection

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

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

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

For details on environment protection, see the section *Protecting Environments*.

Force Impersonation for Natural Development Server

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

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

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

Record Each User's Initial Logon Daily

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

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

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

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

Enable Error Transaction Before NAT1700/1701 Logoff

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

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

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

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

Logoff in Error Case if *STARTUP is Active

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

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

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

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

Set *APPLIC-NAME Always to Library Name

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

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

Allow Deletion of Users Who Are Owners/DDM Modifiers

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

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

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

If this option is set to "O" or "A" and the security profile of a user is deleted, his/her ID is automatically removed from any security profiles where he/she is specified as owner or DDM modifier. Nonetheless, it may be advisable before the deletion to use the Cross-Reference User function to ascertain which profiles/DDMs would be affected, and after the deletion to make sure the changed owner/co-owner and DDM modifier/co-modifier configurations still suit your requirements.

PF-Keys

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

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

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

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

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

PF-Key Functions

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

Key	Function	Explanation
PF01	Help	If you press PF1 on any Natural Security screen, help information for that screen will be displayed.
PF02	Previous Menu	This key returns you to the menu screen from which you have invoked the current processing level. By default, the modifications you made before leaving a function with PF2 will be saved; see also the general option "Exit Functions with Confirmation" above.
PF03	Exit	This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed. By default, the modifications you made before leaving a function with PF3 will be saved; see also the general option "Exit Functions with Confirmation" above.
PF04	Additional Options	On a security profile screen, you can press this key (instead of marking the Additional Options field on the screen with "Y") to display the Additional Options selection window for a security profile.
PF05		Various functions on different screens (as described where appropriate).
PF06	Flip	The PF-key lines at the bottom of the Natural Security screens display either PF-keys 1 to 12 or PF-keys 13 to 24. By pressing PF6, you can switch from one display to the other.
PF07	Previous Page (-)	This key scrolls a displayed list one page backward.
PF08	Next Page (+)	This key scrolls a displayed list one page forward.
PF12	Cancel	This key causes a given processing level to be terminated and the screen of the next higher processing level to be displayed. By default, the modifications you made before leaving a function with PF12 will *not* be saved; see also the general option "Exit Functions with Confirmation" above.
PF13	Refresh	This key undoes all modifications you have made on a screen but which have not yet been saved. The fields on the screen will be reset to the values they had before you changed them.
PF14		(reserved for future use)

Key	Function	Explanation
PF15	Menu	This key invokes the Natural Security Main Menu. By default, the modifications you made before leaving a function with PF15 will be saved; see also the option "Exit Functions with Confirmation" above.
PF16 to PF17		Various functions on different screens (as described where appropriate).
PF18		(reserved for future use)
PF19	First Page (- -)	This key scrolls a displayed list to its beginning.
PF20 to PF24		(reserved for future use)

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

PF09, PF10, PF11, PA1, PA2

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

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

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

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

PF-Key Names

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

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

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

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

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

Logon/Countersign Errors

The Logon/Countersign Errors functions serve two purposes:

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

Logon Errors

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

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

- You can ascertain whether unauthorized people have tried to gain access to Natural.
- You can ascertain what users do wrong when they try to log on. Users may then be informed how to log on correctly.
- You can ascertain whether users have been given the appropriate access rights. A user may, for example, try to log on to an library he/she is not (but should be) allowed to use. In this case you may then make the necessary Natural Security maintenance adjustments to the security profiles and relationships concerned.

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

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

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

Locked Users

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

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

the section *Countersignatures*.)

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

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

How to Invoke Logon/Countersign Errors

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

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

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

- List error entries
- Delete error entries
- Display individual error entries
- List/unlock locked users

The individual functions are described below.

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

Order of Records	• T - The logon error records will be in order of terminal IDs, as defined by the Natural system variable *INIT-ID. For logon errors related to Natural RPC and Natural Web I/O service requests, RPCSRVRQ and NWOSRVRQ respectively will be used instead of the *INIT-ID value. • P - The logon error records will be in order of user IDs, as defined by the Natural system variable *INIT-USER. • TY - Same as "T" for utility access error records. • PY - Same as "P" for utility access error records. This option has no impact on the List/Unlock Locked Users function.
Start Value	If you do not wish to get all, but only a certain range of logon error records or locked users respectively, you may specify a start value as described in the section *Finding Your Way In Natural Security*. Special start values (for Order of Records = T): • RPCSRVRQ - for logon errors which occurred in conjunction with Natural RPC service requests. • NWOSRVRQ - for logon errors which occurred in conjunction with Natural Web I/O service requests.
Date from/to Time from/to	If you wish to get only records of logon/countersign errors that occurred in a specific period of time, you may specify a period of time in these fields.

List Error Entries

This function displays a list of logon error records.

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

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

Delete Error Entries

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

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

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

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

See also the direct command ERRDEL below.

Display Individual Error Entries

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

List/Unlock Locked Users

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

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

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

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

C	Countersign error
L	Logon error

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

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

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

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

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

Deleting All Error Entries - Direct Command ERRDEL

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

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

Logon Records

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

You can specify the option "Logon recorded" in the security profile of each library and each user (see the sections *Library Maintenance* and *User Maintenance* respectively).

A logon record will be written by Natural Security:

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

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

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

Similarly, an access record will be written by Natural Security every time a users invokes a utility in whose default security profile the option "Access recorded" is set to "Y".

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

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

How to Invoke Logon Records

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

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

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

Functions for Logon Records

Each of these functions displays a list of logon records.

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

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

Order of Records	U	List logon records in alphabetical order of user IDs.
	L	List logon records in alphabetical order of library IDs.
	UX	Same as "U", but listing only logon records of undefined users.
	LX	Same as "L", but listing only logon records to undefined libraries.
	Y	List utility access records in alphabetical order of utility names.
	UE	List ETID-related logon records in alphabetical order of user IDs.
	EU	List ETID-related logon records in ascending order of ETIDs.
Start Value	If you do not want a list of all logon records, but would like only certain ones to be listed, you may specify a start value as described in the section *Finding Your Way In Natural Security*.	
Hex	In this field you can specify a start value in hexadecimal format; for example, for ETID-related logon records.	
Date from/to Time from/to	If you wish to view only records of logons which occurred in a specific period of time, you may specify a period of time in these fields. For the function "Delete Logon Records But Last", these fields are ignored.	

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

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

Deleting All Logon Records - Direct Command LOGDEL

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

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

To selectively delete large numbers of logon records, you can use the application programming interface NSCADM.

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

Maintenance Log Records

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

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

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

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

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

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

Display Status of Logging Function

This function displays the following information:

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

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

List Administrator Services Maintenance Logs

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

The log records are listed in chronological order.

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

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

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

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

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

List Security Profile Maintenance Logs

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

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

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

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

The log records are listed in chronological order.

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

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

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

Log File Maintenance

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

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

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

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

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

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

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

Code	Function	Explanation
LI	List Log Records	This function is used to list the contents of the log file. The output contains the same information as displayed by the function List Security Profile Maintenance Logs: a list of all modified profiles/settings, as well as every profile concerned (indicating the profile components which were modified). The output consists of two reports: • the "List of History Log Entries" report will be written to print file CMPRT01, • the "Detail History Log Entries" report will be written to print file CMPRT02.
LX	List Log Records Extended	Same as List Log Records - in addition, this function displays the additional data which are logged if extended logging is activated for user or library profiles; see *Extended Logging* under *Logging of Maintenance Functions*.
WR	Write Log Records to Work File	This function is used to write log records from the log file to Work File 5 (without deleting them from the log file).
WD	Write Log Records to Work File and Delete	This function is used to write log records from the log file to Work File 5, and delete them from the log file.
RA	Read Log Records from Work File	This function is used to read log records from Work File 5 onto the log file.
SA	Scan Work File	This function is used to scan the contents of Work File 5.

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

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

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

For object-type codes of external objects, see Types of External Objects.

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

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

Example:

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

```
LOGFILE
FIN
```

The CMOBJIN batch input file might contain the following specifications:

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

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

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

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

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

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

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

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

//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF,WORK=((5),OPEN=ACC)')
//STEPLIB DD   DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//CMPRINT  DD  SYSOUT=X
//CMWKF05   DD DSN=NSC.LOG.WKF05,
//    DISP=(NEW,CATLG),DCB=(RECFM=VB,LRECL=4624,BLKSIZE=4628),
//    SPACE=(TRK,(5,2))
```

```
//CMSYNIN   DD *
SYSSEC,DBA,password
LOGFILE
22,241
WD,US,,2002-07-01,2002-07-25
.
FIN
/*
//*
```

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

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

```
//DBA       JOB DBA,CLASS=K,MSGCLASS=X
//**
//** LIST LOG RECORDS-WRITE REPORTS OF MAINTENANCE DATA TO PRINTER
//**
//NSCnnBAT EXEC PGM=NATBATnn,REGION=2400K,
// PARM=('IM=D,FNAT=(22,210),INTENS=1,FSEC=(22,240),',
//       'MT=0,MAXCL=0,MADIO=0,AUTO=OFF')
//STEPLIB  DD  DSN=PRODNAT.LOAD,DISP=SHR
//DDCARD   DD  DISP=SHR,DSN=PRD.NATnn.JOBS(ADADB22)
//** CMWKF01   DD DISP=SHR,DSN=NSC.LOG.WKF01
//** CMWKF05   DD DISP=SHR,DSN=NSC.LOG.WKF05
//CMPRINT  DD SYSOUT=X
//CMPRT01  DD SYSOUT=X
//CMPRT02  DD SYSOUT=X
//CMSYNIN  DD *
LOGFILE
FIN
/*
//CMOBJIN  DD *
SYSSEC,DBA,password
22,241
LI,AD,,2002-06-06,2002-06-06
LI,US,MILL*,2002-05-01,2002-05-31
.
/*
//*
```

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

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

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

```
SYSSEC,DBA,password
LOGFILE
22,241
RA,US,,2002-07-01,2002-07-25
.
FIN
/*
//*
```

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

See also the section *Natural Security In Batch Mode*.

List Last Logon Records

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

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

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

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

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

The logon records are listed in chronological order.

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

SAF Online Services

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

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

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

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

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

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

- System Parameters
- System Statistics
- User Statistics
- Zap Maintenance
- Storage Display
- System Tracing
- Refresh Server

System Parameters

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

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

Item	Explanation
Server DBID	Shows the database ID used by the SAF server.
Encrypt Req.	Indicates whether security requests passed between different SAF server components are communicated encrypted.
Encrypt Stg.	Indicates whether storage maintained within the Natural environment is kept in an encrypted state.
Messages	SAF server message level: Level "0" gives only error message, "1" reports security violations and "3" generates an audit trail of all checks.
Cmd Log	Indicates whether command logging is turned on.
Buffer	Indicates whether security checks will be cached by the SAF server.
JCL check	Indicates whether CA-JCL check processing is available within the Natural environment.
Prefix Prog	Indicates whether Natural program names are prefixed with the name of the current application library when performing authorization checks. *Not applicable to Natural SAF Security.*
Protect Obj	Indicates whether program objects are protected within the Natural environment. Users require ALTER access to a particular application in order to modify its program objects. *Not applicable to Natural SAF Security.*
Log SYSMAIN	Indicates whether logging of all SYSMAIN operation is required. *Not applicable to Natural SAF Security.*
SYSMAIN/Lib	Indicates whether authorization checks for SYSMAIN functions will include access to the relevant Natural application libraries. *Not applicable to Natural SAF Security.*
Cmd Line	Indicates whether the Natural command line is protected. Users require CONTROL access in order to enter commands in the Natural command line.
ETID	Indicates whether Natural will generate a unique ETID.
Edit/Lib	Indicates whether Natural will prevent editing of objects located in another Natural application library. *Not applicable to Natural SAF Security.*
Clear/Ed	Indicates whether Natural will clear the edit area when logging onto another Natural application library. *Not applicable to Natural SAF Security.*
Ext Name	Indicates whether Natural will take the user name from SAF. Specifically, the field *USER-NAME will be taken from RACF or CA-ACF2.
Ext Group	Indicates whether Natural will take the group name from SAF. That is, the field *GROUP will be taken from RACF, CA Top Secret, CA-ACF2.
Log API	Indicates whether SMF logging is performed when executing the Natural API.
Env API	Indicates whether authorization checks performed by the Natural API will be prefixed by an environment code based on the Natural system files.

System Statistics

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

Item	Explanation
Authorization	Displays the different resource authorization checks performed by the SAF server related to Natural on mainframes, EntireX Communicator, Adabas, Entire Net-Work and Adabas SQL Server.
Check (+ve)	Indicates the number of authorization checks performed against the security system for each check type. The count indicates authorizations for which access was permitted and can include universal checks.
Check (-ve)	Indicates the number of authorization checks performed against the security system for which access was denied.
Check saved	Shows the number of authorization checks that were optimized by the SAF server because the result was already known.
Overwritten	Number of times positive authorization results were overwritten in the SAF server's cache because more recent information took its place in the buffer. Increase the number of items buffered if this count is excessive for any particular check type.
Lngth	Number of bytes reserved to cache resource profiles belonging to each type of authorization check. This value is generated automatically by the system.
Active Users	Number of users currently active in the SAF server.
High Watermark	High watermark value for number of users present in the SAF server.
Max Users	Maximum of users that can be accommodated.
Overwritten	Number of times a user area was reclaimed and allocated to another user. Increase the total buffer size if this count becomes excessive.
Authenticated	The total number of successful authentication checks performed.
Denied	The number of unsuccessful authentication checks.

User Statistics

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

Zap Maintenance

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

Storage Display

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

System Tracing

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

Refresh Server

This function is used to restart the SAF server.

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

User Default Profiles

Before you use default profiles, you should be familiar with the "normal" way of defining users as explained in the section *User Maintenance*.

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

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

How to Create a Default Profile

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

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

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

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

In this window, enter the following:

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

For information on user IDs and user types, see the section *User Maintenance*.

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

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

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

How to Use a Default Profile

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

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

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

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

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

Library Default Profiles

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

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

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

How to Create a Default Profile

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

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

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

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

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

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

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

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

How to Use a Default Profile

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

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

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

Library and User Preset Values

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

To invoke this function:

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

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

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

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

   With PF5 on the library profile items screen, you can invoke another screen with further library options.

The items are explained below.

Library Profile Items

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

Item	Explanation
Active cross-reference for Predict	Determines whether an active cross-reference in Predict is generated for a library. If you specify an asterisk (*) here, this applies to all libraries: The generation of active cross-references will be determined by the value of the Natural profile parameter XREF, regardless of the "Cross-reference" setting in individual library profiles.
Logon recorded	Determines whether logons to a library are recorded.
Natural programming mode	Determines whether the programming mode can be changed with the Natural profile/session parameter SM. If you specify an asterisk (*) here, this applies to all libraries: The programming mode will be determined by the value of the Natural profile parameter SM, regardless of the "Programming mode" setting in individual library profiles.
Restart	Determines whether an Adabas OPEN command with or without End of Transaction ID (ETID) is executed during the logon procedure.
Maintenance with Natural utilities	Determines who may maintain the contents of the library with Natural utilities.
Clear source area by logon	Determines whether the editor’s source work area is cleared automatically when a user logs on from the library to another library.
Execute startup transaction in batch	Determines whether the startup transaction specified in the library profile is executed in batch mode.
Steplibs	Allows you to specify the libraries which are to be the steplib libraries for the library. You can specify the name of the first steplib in the Steplibs field on the Preset Library And User Values screen. To specify more than one steplib, enter an asterisk (*) in the field or press PF4: a window will be displayed, in which you can specify up to 9 steplibs.

Item	Explanation
Profile parameters for undefined libraries	This is an option which applies to undefined libraries in general. For libraries for which no security profiles have been defined yet, the following settings will be determined by the corresponding Natural profile parameters: **NC** Allow system commands.
RPC Server Session Options (Natural RPC Restrictions)	
Close all databases	Controls the logon-/logoff-dependent closing of databases opened by remote subprograms in a library.
Logon option	Determines which logon data are evaluated when a library is accessed via a Natural RPC service call.
Logon recorded	This is not only a preset value. It also applies as default value if the corresponding field in the library profile is set to "*". If this is the case, it determines whether access to a library is to be recorded or not when the library is accessed via a Natural RPC service call.
Lock user option	This is not only a preset value. It also applies as default value if the Lock User option in the security profile of the Natural RPC server is set to "*". If this is the case, it controls the locking of users when they attempt to access a library on that server via a Natural RPC service call: **N** No locking of users will be performed. **X** Once a user has reached the maximum number of logon attempts without supplying the correct password, he/she will be locked, that is, the user ID will be made "invalid". Natural Security "remembers" unsuccessful attempts across sessions: The error counters for the client user IDs which were tried out unsuccessfully are kept for access attempts in subsequent sessions, thus reducing the number of subsequent attempts with these IDs. The error counter for a user ID is only reset after a successful logon. ***** The locking of users is controlled by the Lock User Option in the General Options section of Administrator Services. For details on this feature, see also the Lock User Option under *General Options*.

Further Library Options

Module Protection Mode

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

*****	The evaluation of the Disallowed/Allowed settings depends on the platform: • **On mainframe computers:** When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is only evaluated if the module is contained in that library. • **On other platforms:** When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is *always* evaluated, regardless of whether the module is contained in the current library or another library (steplib).
L	The evaluation of the Disallowed/Allowed setting is the same on any platform: When a module is invoked for execution, the Disallowed/Allowed setting for this module in the current library's security profile is only evaluated if the module is contained in that library. Setting this option to "L" may be useful if you transfer a Natural application from a mainframe to a non-mainframe platform and wish to keep you module protection unchanged.

Disable Rename and Delete of Library Node

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

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

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

NDV Startup Inactive

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

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

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

User Profile Items

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

Item	Explanation
ETID	You may specify which value is to be used as ID for End of Transaction data (ETID). For Natural Security to be able to supply ETIDs, the Natural session must be started with the Natural profile parameter ETID being set to "OFF" or its default value. **S** This setting applies to all users; it cannot be changed in individual user profiles. An ETID for every user will be generated by Natural Security at the start of the his/her Natural sessions. Such an ETID consists of "S", followed by a time-stamp (the leftmost 7 bytes of the value of the Natural system variable *TIMESTMP at session start), and uniquely identify the user session. It will remain in effect until the user ends his/her Natural session. In the individual user profiles, this is indicated by the Default ETID field being prefixed with "S>"; any not time-stamp-related ETID value shown in that field will then not be used. To use a time-stamp-related ETID for a single user only, you specify `*TIMSTMP` in the Default ETID field of the individual user profile. If time-stamp-related ETIDs are used, a logon record containing the ETID will be written by Natural Security every time a user logs on to Natural. To ascertain which ETID has been used by which user ID, you can view the logon records, or use the application programming interface NSCADM. For service requests in an RPC client/server environment, you can also use time-stamp-related ETIDs; see Components of an RPC Server Profile. **Note:** With ETID=S, the Natural system variable *ETID contains binary, non-printable data; this may affect your applications if they evaluate the *ETID value. For the display, you may consider using an edit mask; e.g. EM=(H(8)). **G** ETIDs will be generated by Natural Security during the logon procedure from the following components: ● The 1st byte is single character that identifies the environment from which Natural is invoked (B=Batch, C=Color, P=PC, T=TTY, V=Video, X=BTX). ● The 2nd to 5th bytes is a unique string of alphanumeric characters that identifies the user (this string is generated when a user is defined to Natural Security). Only these 4 bytes are displayed in the user's security profile. ● The 6th to 8th byte is a unique string of alphanumeric characters that identifies the library (this string is generated when a library is defined to Natural Security). **U** The ID by which a user is defined to Natural Security, i.e. the value of the Natural system variable *USER, will be used as ETID. If the Automatic Logon feature (which is described in the section *Logging On*) is used, the value of *USER will be identical to that of *INIT-USER. **I** The value of the Natural system variable *INIT-USER will be used as ETID. **T** The value of the Natural system variable *INIT-ID will be used as ETID. **N** ETIDs will not be used. If you do not remember the possible values you may specify, enter a question mark (?) or an asterisk (*) in the field: a window will be displayed; in the window, mark the desired value with a character or with the cursor; the value will then be written into the ETID field. See the Natural *System Variables* documentation for details on the above-mentioned system variables.
Private library for administrator/person	Determines whether the user, if he/she is of type PERSON or ADMINISTRATOR, may have a personal ("private") library.

Item	Explanation
Message before password expiration	This option applies to user profiles in general. You can use it to have a message displayed to users whose password is about to expire. The number you specify here - possible values are 1 to 10 - determines how many days before his/her password expiration is due a user is to a receive message, indicating that his/her password will expire. The message (NAT1691) will be displayed after the initial logon to Natural. This only applies to users in whose security profiles a time interval for password change is set (option "Change after *nnn* days" in a user profile.)
Minimum password length	This option applies to user profiles in general. A user password must not consist of fewer characters than the number specified here. Possible values are 1 to 8. When you set this length, please bear in mind that by default passwords are identical to user IDs (see the section *User Maintenance*).
Password case-sensitive	This option applies to user profiles in general. It determines whether or not Natural Security is to distinguish between lower-case and upper-case characters in user passwords: **N** Natural Security internally converts all alphabetical characters in passwords to upper-case. **Y** Natural Security distinguishes between lower-case and upper-case characters in passwords. See also *Password Rules* below. **Note:** If you set this option to "Y", make sure that any password input fields used also distinguish between lower-case and upper-case. This may affect the logon screen, the user exit LOGONEX1, any logon-related Natural Security application programming interfaces, or Natural's RPC-logon-related application programming interfaces.
User password history	This field corresponds to the general option User Password History.

Password Rules

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

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

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

Minimum no. of lower-case letters	In this field, you can specify how many lower-case alphabetical characters passwords must contain at least.
Minimum no.of non-letters	In this field, you can specify how many non-alphabetical characters passwords must contain at least.

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

Definition of System Libraries

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

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

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

To define system libraries:

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

   The Administrator Services Menu will be displayed.

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

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

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

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

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

Definition of Undefined Libraries

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

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

To define undefined libraries:

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

   The Administrator Services Menu will be displayed.

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

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

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

3. Proceed as described under *Listing Undefined Libraries* in the section *Library Maintenance*.