Natural Security

The enhancements listed in this chapter are available with Natural Security Version 6.3. The following topics are covered:

- General Information
- Administrator Services
- User Profiles
- Library Profiles
- Utility Profiles
- RPC Server Profiles
- Application Programming Interfaces
- SECULD2/SECLOAD Transfer Programs
- Logon Procedure
- Functional Security
- Limitations on OpenVMS

General Information

The following topics are covered below:

- FSEC System File
- Shared FSEC System File
- Concurrent Modifications of a Security Profile
- WYSIWYG
- Direct Commands
- Link Functions

FSEC System File

With version 6.3, you can continue to use your existing FSEC system file. No migration of Natural Security data from the previous version to the current version is necessary.

Shared FSEC System File

If you use an FSEC system file shared by multiple versions of Natural Security, be aware that the new features described below are not available with versions prior to 6.3 for Windows and UNIX and 4.2.4 for mainframe platforms.

Concurrent Modifications of a Security Profile

A new general option **Concurrent Modifications Without Notification** allows you to determine how Natural Security is to react 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 This means that, at this point, Administrator 2 is working on data which are "out of date", but is not aware of this fact.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. Depending on the setting of the new general option **Concurrent Modifications Without Notification**, 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.

WYSIWYG

If you use functional security within Natural Security, that is, if you use the command processor NSCCMD01 to disallow functions within the library SYSSEC, this now has a "WYSIWYG" effect: If functions are disallowed in NSCCMD01, the corresponding menu items will not be visible on the Natural Security menus. This means that within SYSSEC, you will only see the functions you are allowed to use.

Direct Commands

As of this version, you can also issue a Natural Security direct command from outside of the Natural Security library SYSSEC. This allows you to perform a Natural Security function from anywhere in your Natural session without having to log on to the library SYSSEC. To do so, you enter the direct command - prefixed by "SYSSEC" - in the Natural command line. After the function invoked by the direct command has been performed, you will be returned to the Natural screen from which you have issued the command.

The following new direct commands - and keywords in NSCCMD01 - are available to invoke Administrator Services functions directly:

New Direct Command	Function Invoked
ADMIN_D	Library And User Preset Values
ADMIN_I	Application Programming Interfaces
ADMIN_N	Maintenance Log Records
ADMIN_S	System-Library Definitions
ADMIN_U	User Default Profiles
ADMIN_X	Utility Defaults/Templates
ADMIN_Y	Library Default Profiles
ADMIN_1	Environment Profiles

Link Functions

With earlier versions, when you invoke a function for the maintenance of links, you would get a list of all objects to which the selected object can be linked, that is, those for which links already exist and those for which not.

As of this version, a new option **Select only defined links** is provided; it allows you to display either a list of all linkable objects or a list of only those objects which are already linked. This new option is available for all link maintenance functions; it appears in the window displayed when you invoke a link function.

Administrator Services

The following enhancements are provided:

- New General Options
- Logon Records
- Logon/Countersign Errors
- System-Library Definitions
- Environment Protection

New General Options

Record Each User’s Initial Logon Daily

The new general option **Record Each User’s Initial Logon Daily** 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.

When this option is active, the new application programming interface NSCXRUSE (see below) can be used to obtain a list of users who have not logged on since a specified date.

Allow Deletion of Users Who Are Owners/DDM Modifiers

With previous versions, it was not possible to delete a user profile as long as the user was specified as owner or DDM modifier in any security profile.

As of this version, you can use the new general option **Allow Deletion of Users Who Are Owners/DDM Modifiers** to determine whether or not the security profile of a user who is owner or DDM modifier can be deleted.

Generation of ETIDs

The **ETID** option in the **Library and User Preset Values** has been enhanced: The new setting "S" causes an ETID to be generated by Natural Security for every user at the start of his/her Natural session. The ETID contains a time-stamp component, which makes it unique, and it will remain in effect for the entire session. See *Library and User Preset Values* in the *Natural Security* documentation for details.

A similar option **Time-Stamp-Related ETID** is available for Natural RPC servers (see below).

Profile Parameter Override of Library-Profile Settings

For the following **Library and User Preset Values**, an additional option is available: **Active cross-reference for Predict** and **Natural programming mode**. You can specify an asterisk (*) instead of their other possible values. This will then apply to all libraries as follows:

- 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.
- 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.

Profile Parameters for Undefined Libraries

A new **Library and User Preset Values** option, **Profile parameters for undefined libraries**, is available. Provided that the general option **Transition Period Logon** is set to "Y", this new option applies to all libraries for which no security profiles have been defined yet. If you set it to "Y", the permission to use Natural system commands (which for defined libraries is determined by the security option **Allow system commands** in the library profiles) will be determined by the Natural profile parameter `NC`.

Set *APPLIC-NAME Always to Library Name

With previous versions, the Natural system variable `*APPLIC-NAME` either contained the name of the library to which the user was logged on, or, if the user was logged on via a special link, the special-link name.

With this version, a new general option **Set *APPLIC-NAME always to library name** is available. It can be set so that `*APPLIC-NAME` always contains the library name, regardless of whether the user is logged on via a special link or not.

Mailboxes in Batch Mode

With previous versions, mailboxes are not output in batch mode.

With this version, a new general option **Suppress mailboxes in batch mode** is available. It determines whether mailboxes are output in batch mode or not.

Logon Records

Similar to logon records for users and libraries, it is now possible to write records when users invoke a utility. The writing of such utility access records is activated by the new session option **Access Recorded** in the utility’s default profile (see below). The records can be reviewed with the **Logon Records** function.

Logon/Countersign Errors

The **Logon/Countersign Errors Menu** provides the new selection options **Date from/to** and **Time from/to**: They allow you to restrict the range of error records to which a function is applied to logon/countersign errors which occurred in a specific period of time.

Moreover, the selection option **Order of Records** has been enhanced: In addition to logon and countersign errors, you can select utility access errors.

The functions for the handling of logon/countersign error records have been enhanced. They allow you to selectively handle logon errors which occurred in conjunction with Natural RPC service requests and Natural Web I/O service requests. To do so, you specify the following in the **Start Value** field on the **Logon/Countersign Errors Menu**:

- RPCSRVRQ - for logon errors in conjunction with Natural RPC service requests.
- NWOSRVRQ - for logon errors in conjunction with Natural Web I/O service requests.

System-Library Definitions

Several new system libraries (that is, libraries whose names begin with "SYS") are provided with this Natural version. They are included in the list of libraries provided by the Administrator Services function **System-Library Definitions**, which you can use to automatically create security profiles for them.

Environment Protection

With this version, Natural Security allows you to make users’ access to a library environment-specific. A Natural environment is determined by the combination of the system files `FNAT`, `FUSER`, `FSEC` and `FDIC`. You define a security profile for each environment (that is, for each system-file combination) you wish to protect, and control users’ access to it. You can also make a library accessible in some environments, but not in others.

Whenever a user logs on to a library in another environment, Natural Security will check whether:

- access to the library is allowed in that environment, and
- the user is authorized to access that environment.

Such a check is performed not only when a user explicitly logs on to a library, but also when the user invokes a function which implicitly accesses another library or processes the contents of another library.

Environment protection is activated with a new general option **Environment Protection**. When environment protection is active, the following applies:

- Access to undefined environments is not possible.
- For every environment to be accessed, an environment security profile has to be defined.
- By default, access to a library is allowed in any defined environment, and access to a defined environment is allowed for all users.
- For individual libraries and users, you can disallow access to a defined environment.

See the section *Protecting Environments* in the *Natural Security* documentation for details on environment protection.

Note:
The above-mentioned environment-protection functionality replaces the Administrator Services function **Definition of System-File Access** which was available with earlier versions of Natural Security.

User Profiles

Copying User’s Links

The new user maintenance function **Copy User’s Links** allows you to copy links which are defined for one user profile to another existing user profile. The function allows you to individually select the links you wish to copy.

Library Profiles

The following enhancements are provided:

- Private Libraries
- Linking Administrators to an Unprotected Library
- Copying Libraries
- Copying, Renaming and Deleting Libraries
- Default Profiles
- Statement and Command Restrictions
- Library SYSEXRM
- Copy Library Profile

Private Libraries

With earlier versions, access to a private library is restricted to the user for whom the private library is defined.

As of this version, it is possible to remove this restriction and control access to private libraries in the same way as access to other "normal" libraries.

With the new general option **Private Libraries in Public Mode**, you can choose "public mode". In this mode, private libraries are handled like any other libraries:

- You can choose not to protect a private library, which means that it can be accessed by any user.
- You can make a private library protected, which means that it can only be accessed by the user whose ID is the same as the library ID, and by users who are linked to it.

For details, see the description of the additional option **Private Library** in *Components of a User Profile*, which can be found under *User Maintenance* in the *Natural Security* documentation.

In private mode, private libraries continue to be maintained in the user maintenance section of Natural Security; in public mode, private libraries are maintained in the library maintenance section.

Linking Administrators to an Unprotected Library

With earlier versions, it is not possible to establish a link between a user and an unprotected library. The conditions of use of the library are determined by the library profile.

As of this version, it is possible to establish a special link between a group and an unprotected library. This special link applies only to administrators contained in that group. Thus it is possible to define special conditions of use for administrators if this should be required for administration or maintenance tasks. For this purpose, the protection combination in the library profile has to be set to "People-protected=L, Terminal-protected=N".

Copying Libraries

The Copy Library provides a new option **with links**. It allows you to copy not only the library profile, but also existing links associated with that library profile.

Copying, Renaming and Deleting Libraries

With earlier versions, when you copy, rename or delete a library security profile, this has no effect on the library itself and its contents stored on the `FUSER` system file.

As of this version, the functions **Copy Library**, **Rename Library** and **Delete Library** provide a new option **with Natural objects** which allows you to also adjust the `FUSER` system file accordingly when a library profile is copied, renamed or deleted, which means that the contents of the library on the `FUSER` file are also copied to another library, moved to another library, or deleted.

Default Profiles

With earlier versions, default security profiles can only be defined for users. As of this version, you can also define default profiles for libraries.

Statement and Command Restrictions

The use of the new statements and system commands provided with the current version of Natural can also be controlled with Natural Security.

The following commands have been removed: `ADHOC`, `CREATE`, `GRAPHICS` and `IDL`.

Library SYSEXRM

The Natural example library `SYSEXRM` is now called `SYSEXSYN`. If you have a library profile defined for `SYSEXRM`, you should therefore rename it to `SYSEXSYN`.

Copy Library Profile

When you use the **Copy Library** function to copy a library profile, the **Free List of Modules** (which is obtained by pressing PF9 on the **Disallow/Allow Modules** screen of a library profile) is copied as well. With previous versions, the list was not copied.

Utility Profiles

The following enhancements are provided:

- Session Options
- SYSDDM
- SYSOBJH - Object Handler
- NATLOAD, NATUNLD, SYSTRANS

Session Options

The **Additional Options** section of the default utility profiles has been enhanced to provide the following session options:

Option	Explanation
Access Recorded	This option allows you to record access to a utility. It corresponds to the option **Logon Recorded** in user and library profiles. When a user invokes a utility, a record will be written. The **Logon Records** function of Administrator Services can be used to view these records.
Privileged Groups	This option may be used to influence the order in which Natural Security searches for the appropriate utility profile to apply. It determines whether or not utility profiles defined for the "privileged groups" (which are specified in a user security profile) will become part of the search order.
*GROUP Only	When a user invokes a utility function and Natural Security searches for appropriate utility profile to be applied, the search sequence, by default, includes user-library-specific and user-specific utility profiles of all groups in which the user is contained. With this option, you can restrict the search to utility profiles of the current group (as determined by the current value of the Natural system variable `*GROUP`) and exclude the utility profiles of other groups from the search sequence. See the section *Which Utility Profile Applies?* in the *Natural Security* documentation for details.
MAINUSER API	This option (which is only available for the `SYSMAIN` utility) controls the use of `SYSMAIN` functions invoked via the application programming interface `MAINUSER`. It allows you to create a separate set of utility profiles to allow/disallow the use of `SYSMAIN` functions when invoked via the `MAINUSER` API. These profiles are independent of the "normal" `SYSMAIN` utility profiles which control the use `SYSMAIN` functions when invoked via the `SYSMAIN` command.
Utilities option	This this option is only available for the Object Handler (`SYSOBJH` utility). It can be used to make the **Utilities** option in library profiles apply to `SYSOBJH`.

SYSDDM

As of this version, the use of the `SYSDDM` utility can be controlled by Natural Security utility profiles not only for Natural on mainframe computers, but also for Natural on UNIX and OpenVMS.

Note:
With one of the next releases, `SYSDDM` utility profiles will also be applicable to Natural on Windows.

SYSOBJH - Object Handler

The utility profiles for `SYSOBJH` (Object Handler) provide the following enhancements:

- The Unload, Load and Delete functions can be allowed/disallowed selectively for mainframe DDMs, mainframe-related objects, and applications.

- The `REPLACE` parameter can be allowed/disallowed selectively for the Load function in user-library-specific profiles.

The initialization of the Natural utility `SYSOBJH` (Natural Object Handler) under Natural Security has been improved to make the use of the utility more user-friendly: With previous versions, users were not notified that they were not allowed to use a selected function/option until they actually attempted to execute it. Now a disallowed function/option is intercepted at the earliest possible stage in the selection process.

NATLOAD, NATUNLD, SYSTRANS

The Natural utilities `NATLOAD`, `NATUNLD` and `SYSTRANS` are no longer available (see also *Removed Features*). For compatibility reasons, however, utility protection for them is still possible: If utility profiles for these utilities already exist, you can continue to define and maintain them. If none exist, utility profile maintenance for these utilities will be disabled.

Note:
`NATLOAD` and `NATUNLD` were only available on mainframe, UNIX and OpenVMS platforms.

RPC Server Profiles

The following enhancements are provided:

- Time-Stamp-Related ETID
- Single-Library RPC Servers

Time-Stamp-Related ETID

The new option **Time-Stamp-Related ETID** allows the generation of time-stamp-related ETIDs for RPC server sessions, in the same way as described above for user session (see *Generation of ETIDs* above).

Single-Library RPC Servers

For Natural RPC servers which provide services performed by subprograms contained in a single library, a new option **Logon Mode** is available. It can be specified in the security profiles of Natural RPC servers to improve performance.

Setting the option to "S" (Static Mode) has the following effects:

- The library on the server is set at the start of the server session, and will remain unchanged until the end of the server session.
- The server will process only service requests for this library. Service requests for any other library will be rejected.
- If the library is unprotected (People-protected = N), the user’s authorization to access the library is not checked. If the library is protected (People-protected=Y), the user’s authorization to access the library is checked.
- After a successful check, the user’s conditions of use of the library are determined by the library profile. Even if a special link exists between the user and the library, any settings in the special link profile will be ignored.

See the section *Validation of an RPC Service Request* in the *Natural Security* documentation for details.

Application Programming Interfaces

The following enhancements are provided:

- Enhancements to All APIs - Error Texts
- New APIs
- Enhanced APIs

Enhancements to All APIs - Error Texts

All Natural Security application programming interfaces (APIs) have been enhanced: In the case of an error, they now provide the option to return not only the error message number, but also the associated error text. For details, see the parameter descriptions in the source codes of the API examples provided in the library SYSSEC.

New APIs

As of this version, "interface subprograms" are called "application programming interfaces".

The following new application programming interfaces (APIs) are provided:

API	Function
NSCADM	This application programming interface is used to: ● Display the settings of General Options in Natural Security's Administrator Services. ● List and delete logon records. See the example program PGMADM02 in the library SYSSEC for details. ● Remove/re-establish Natural Security's security profile maintenance/retrieval sections for base/compound applications and RPC servers. See the example program PGMADM03 in the library SYSSEC for details.
NSCXRUSE	This application programming interface is used to: ● Display users whose number of unsuccessful logon attempts is greater than "0". ● Display users who have not logged onto Natural since a specified date. See also *Record Each User's Initial Logon Daily* above.
NSCXLO	This application programming interface is used to read the maintenance log records which are created by Natural Security if the general option **Logging of Maintenance Functions** has been activated.
NSC---P	This application programming interface is used for password verification.
NSC----P	This application programming interface is used for password verification and password change.
NSCXRIER	This application programming interface is used to display individual logon error records.

Enhanced APIs

The following application programming interfaces (APIs) have been enhanced:

API	Function
NSC---L	This application programming interface now allows you to ascertain which modules in a library are available to a user. For details, see the example program PGM---LM in the library SYSSEC.
NSCUS	With previous versions, when you used the application programming interface NSCUS to modify the owner specifications in a user profile, any existing owner specifications in the profile were overwritten by the newly specified ones. As of this version, NSCUS allows you to choose between either overwriting the existing owners entries or appending the new owner entries to the existing ones without overwriting them.
NSCXR	This application programming interface now allows you to do the following: ● Retrieve the user ID belonging to a specified user name. For details, see the example program PGMXR014 in the library SYSSEC. ● List all libraries of the current FNAT or FUSER system file which are not defined in Natural Security. For details, see the example program PGMXR015 in the library SYSSEC. ● Translate the 2-character object-type code into the corresponding object type. For details, see the example program PGMXR016 in the library SYSSEC. ● Display a list of users who are linked to an external object. For details, see the example program PGMXR017 in the library SYSSEC.

SECULD2/SECLOAD Transfer Programs

The following enhancements are provided:

- SECULD/SECULD2
- New Features for SECULD2
- Conversion Table and EBCDIC-ASCII Conversion
- Batch Processes

SECULD/SECULD2

SECULD2, which is a copy of SECULD with additional functionality, provides enhanced selection criteria to determine the range of objects to be unloaded.

It is recommended that you use SECULD2 instead of SECULD. SECULD will be removed in a future version.

New Features for SECULD2

New Option

SECLOAD provides a new option **Simulate Loading** which allows you to ascertain whether all data from the work file can be loaded to the system file, before you actually load them.

Enhanced Selection Criteria

With some SECULD functions, asterisk notation cannot be used in the **Start Value** field, for example, functions related to external objects. The reason is that asterisk notation would not work with external objects, where an asterisk (*) can be a valid character as part of the object ID itself.

For the sake of consistency, asterisk notation for any function or any object type is no longer possible in the **Start Value** field. Instead, an additional **Range** field is provided, which allows you to determine how the value you specify in the **Start Value** field is to be treated. Three options are possible:

- The range of objects begins with the one whose object ID begins with the Start Value ("genuine" start value).
- The range of objects comprises only those whose IDs begin with the Start Value (corresponds to asterisk notation).
- The range of objects comprises only the one object whose ID is specified as Start Value.

For the unloading of links between users and objects (function code "L"), an additional selection criterion can be specified to determine the range of links to be unloaded: A new field **Link ID** is provided, where you can specify a user ID to unload only links of a certain user or range of users.

A second **Range** field is provided, which allows you to determine how the value you specify in the **Link ID** field is to be treated. Its options are in analogy to those of the Start Value’s **Range** field.

For function code "L", the **Start Value** and **Link ID** fields, and their corresponding **Range** fields, can be used in combination with one another.

Conversion Table and EBCDIC-ASCII Conversion

With previous versions, SECULD/SECLOAD used the corresponding unload/options of the SYSTRANS utility for character conversion. With the new version of SECULD2/SECLOAD, an API subprogram NSCCONV in the library SYSSEC is provided for this purpose. You can adjust the source of this subprogram to suit your requirements.

Batch Processes

The new unloading program with the enhanced functionality as described above is called SECULD2. This means that you have to adjust your batch processes to invoke SECULD2 instead of SECULD.

To ease the transition, the old SECULD program is - for the time being - still available in the library SYSSEC. It will be removed in a future version of Natural Security.

Logon Procedure

The following enhancements are provided:

- Unsuccessful Logon Attempts
- Password Expiration Message

Unsuccessful Logon Attempts

As of this version, the number of unsuccessful logon attempts is passed as a parameter to the logon-related user exit `LOGONEX1`. Thus, it is possible, for example, to display corresponding information to the user before the maximum number of logon attempts is reached. For details, see the source of `LOGONEX1`.

Password Expiration Message

As of this version, you can issue a warning message "Your password will expire on date" (NAT1691) to users at the initial logon. The output of this message is activated with the new option **Message Before Password Expiration** in Administrator Services.

Functional Security

Status of Command Processor

If the status of a command processor is "modified" (that is, modified with `SYSNCP`), you have to update the functional security defined in Natural Security for the command processor. With earlier versions, you have to make this adjustment for each command processor individually. As of this version, the new function `UC` of application-interface subprogram `NSCLI` allows you to simultaneously update the functional security of all "modified" command processors in a library.

Limitations on OpenVMS

In some places, the documentation set for Natural for OpenVMS mentions features which are (currently) not supported with Natural for OpenVMS. Such features are:

- Enable Error Transaction Before NAT1700/1701 Logoff
- Suspend Line Protection
- Time Differential and Time Zone
- Adapters
- Support of Integrated Authentication Framework

Enable Error Transaction Before NAT1700/1701 Logoff

Restricted to mainframes.

The new general option **Enable Error Transaction Before NAT1700/1701 Logoff** allows you to have the current application's relevant `ON ERROR` statement and/or error transaction (`*ERROR-TA`) processed in the case of Natural errors NAT1700 (time window exceeded) and NAT1701 (non-activity time limit exceeded). This option only applies on mainframe computers; on non-mainframe platforms, its setting has no effect.

Suspend Line Protection

Restricted to Windows.

The Natural Studio program editor function **Suspend Line Protection** can be allowed/disallowed in the Session Options section of user security profiles.

Time Differential and Time Zone

Restricted to mainframes.

With earlier versions, the **Time Differential** option in user security profiles is only available for users of type TERMINAL.

As of this version, it is also available for GROUPs. In addition, a new option **Time Zone** is provided, which can be used as an alternative to **Time Differential**.

Adapters

Restricted to Windows.

The use of the new Natural object type "adapter" can also be controlled by Natural Security: This is done by allowing/disallowing the editing of the object type "adapter" in the **Editing Restrictions** section of library profiles.

Support of Integrated Authentication Framework

Restricted to Non-OpenVMS environments.

As of this version, Natural Security supports Natural RPC servers which use an Integrated Authentication Framework (IAF) server for token validation. See also *Limitations on OpenVMS* in the RPC section of these *Release Notes*.

See the section *IAF Support* in the *Natural Security* documentation for details.