Release Information for Natural Version 6.3.5

This chapter covers the following topics:

- New Features
- Changes and Enhancements
- Known Issues
- Natural Remote Procedure Call (RPC)
- Natural Security
- Documentation

New Features

Parameters

The following new Natural parameters are provided in this version:

Parameter	Description
RPCSDIR	Specifies the name of the Natural library in which the service directory is located.
SRVCMIT	Specifies the time at which a Natural RPC server automatically commits an RPC conversation or a non-conversational RPC request.
SRVTERM	Specifies the event at which a Natural RPC server is automatically terminated.

Application Programming Interfaces

The utility SYSEXT provides the following new application programming interfaces (APIs):

API	Description
USR4005N	Read current PF-key settings.
USR4212N	Read a data area from the system file/file system and return the single entries in a table. This allows you to analyze a data area independent of the way the definitions were done in the data area editor. It also allows you to process data areas in DEFINE DATA format.
USR6304N	Set/get the reliable state for the reliable Natural RPC.
USR6305N	Commit/rollback reliable RPC message(s). This API is required if the reliable RPC state has been set to "client commit".
USR6306N	Retrieve the status of all reliable RPC messages of the user who is currently logged on to the EntireX Broker.

Configuration Tool for the Natural Web I/O Interface Client

A configuration tool is now available on J2EE servers. It is used to manage the contents of the configuration files for the session (*sessions.xml*) and for logging (*natlogger.xml*). See *Using the Configuration Tool* in the *Natural Web I/O Interface* documentation.

Changes and Enhancements

Configuration Utility

Remote Procedure Call

The new profile parameters RPCSDIR, SRVCMIT and SRVTERM can be specified. See *Remote Procedure Call* in the *Configuration Utility* documentation.

Session Configuration for the Natural Web I/O Interface Client

A number of features that was previously controlled by an XSLT file (colors, fonts, PF key buttons) is now controlled by a style sheet (CSS). As of this version, the XSLT file only provides restricted possibilities (see *Modifying the Field Attributes* in the *Natural Web I/O Interface* documentation). The XSLT files of the previous versions are no longer supported.

Note:
As of version 6.3.7, the above chapter is no longer available.

The new URL parameter natparamext extends an existing Natural parameter definition in the configuration file. The extension works in the following way: the Natural parameters defined in the configuration file come first. Then, the Natural parameters defined in the URL parameter natparamext are added, separated by a space character. If you want to overrule the definition in the configuration file, use the URL parameter natparam instead. See *Starting a Natural Application with a URL* in the *Natural Web I/O Interface* documentation.

It is now possible to define the following new settings in the configuration file for the sessions. The headings below correspond to the options that are used in the new configuration tool (see *Overview of Session Options* in the *Natural Web I/O Interface* documentation). These new options are only available for J2EE servers, not for IIS.

Use SSL

You can enable SSL. A secure connection is then established between the Natural Web I/O Interface client on the application server and the Natural Web I/O Interface server.

Corresponds to the `ssl` attribute of the `session` element in *sessions.xml*.

Show function key numbers

You can determine whether the PF key numbers are shown next to the PF keys.

Corresponds to the `showfkeynumbers` attribute of the `screen` element in *sessions.xml*.

It is now possible to specify a trust file in the configuration file for the sessions. Trust files are used for a secure connection between the Natural Web I/O Interface server and the Natural Web I/O Interface client. The headings below correspond to the options that are used in the new configuration tool (see *Global Settings* in the *Natural Web I/O Interface* documentation). These new options are only available for J2EE servers, not for IIS.

SSL trust file path

The path to your trust file. For further information, see *Trust Files (J2EE only)* in the *Natural Web I/O Interface* documentation.

Corresponds to the `trustfile_name` element of the `global` section in *sessions.xml*.

SSL trust file password

If your trust file is password-protected, the appropriate password is required.

Corresponds to the `trustfile_password` element of the `global` section in *sessions.xml*.

Known Issues

The information provided for Version 6.3.4 in the section *Known Issues* still applies for Version 6.3.5. In addition, the following applies:

EntireX Broker Stub for Natural Remote Procedure Call (RPC)

Natural Remote Procedure Call (RPC) cannot be used until the EntireX Broker Stub is available.

Support of Integrated Authentication Framework (IAF) on Server Side

The Integrated Authentication Framework cannot be used by a Natural RPC server until the EntireX Broker Stub is available.

Natural Remote Procedure Call (RPC)

Natural Remote Procedure Call (RPC) is available as a separate subcomponent of Natural. It has its own version number. This measure takes into account that Natural RPC is a cross-platform component and makes it possible to provide new Natural RPC versions independent of new Natural versions for the various platforms supported.

With Natural Version 6.3.5, an enhanced Natural Remote Procedure Call Version 6.3.2 is delivered that replaces the existing Natural RPC Version 6.3.1.

See also *Known Issues* above.

As of Version 6.3 of Natural Remote Procedure Call (RPC), the following changes, enhancements and new features are provided:

- Profile Parameters
- Reliable RPC
- Support Logging and Accounting of RPC Program and RPC Library within the EntireX Broker
- Availability of *SERVER-TYPE=RPC Enhanced
- Dynamic Resize of Buffer (MAXBUFF)
- New RPC-Specific Application Programming Interfaces
- Support of Integrated Authentication Framework (IAF) on Server Side

Profile Parameters

The following new profile parameters are available:

- `SRVCMIT` - Server Commit Time
- `SRVTERM` - Server Termination Event
- `RPCSDIR` - Library for Service Directory

The following profile parameter has been changed:

- `MAXBUFF` - Maximum Buffer Size

Reliable RPC

Reliable RPC is the Natural RPC implementation of a reliable messaging system. It combines the Natural RPC technology and persistence, which is implemented by means of units of work that are offered by the EntireX Broker. Reliable RPC is characterized by following features:

- The Natural RPC client executes a `CALLNAT` statement without waiting for a reply from the server (the RPC message is sent in asynchronous mode).

- An RPC server needs not be active at the time the CALLNAT is executed.
- The reliable RPC message is stored in the Broker's persistent store until an RPC server is available.
- The Natural RPC server executes the reliable RPC by calling the requested subprogram but does not send a reply to the RPC client.
- A Natural RPC client may ask the status of the sent reliable RPC messages.
- A Natural RPC client may send a reliable RPC message to an EntireX RPC server.
- A Natural RPC server may receive a reliable RPC message from an EntireX RPC client.

For further information, see *Reliable RPC* in the *Natural Remote Procedure Call (RPC)* documentation.

Support Logging and Accounting of RPC Program and RPC Library within the EntireX Broker

The Natural RPC client provides the name of the subprogram that is to be executed and the name of the library from which the subprogram is to be executed to the EntireX Broker.

The Natural RPC server returns the name of the subprogram that has been executed and the name of the library from which the subprogram has actually been executed.

For further information, see *EntireX Broker Support* in the *Natural Remote Procedure Call (RPC)* documentation.

Availability of *SERVER-TYPE=RPC Enhanced

The Natural RPC server shows the system variable content *SERVER-TYPE=RPC already during the processing of the commands that have been placed on the Natural stack with the Natural profile parameter STACK. With this enhancement, all Natural objects that are executed by the Natural RPC server can check the system variable *SERVER-TYPE for RPC.

In previous versions, *SERVER-TYPE=RPC was only available during the execution of an RPC request.

Dynamic Resize of Buffer (MAXBUFF)

The size of the buffer which is used to exchange data between client and server will be dynamically increased on demand. The size specified with the profile parameter MAXBUFF is used as default value.

This measure will avoid most Natural errors that are reported with Natural error message NAT6964 and reason codes 4, 5 and 7.

New RPC-Specific Application Programming Interfaces

The following RPC-specific application programming interfaces have been added:

- USR6304N - Set/get the reliable state for the reliable Natural RPC
- USR6305N - Commit/rollback reliable RPC message(s). This API is required if the reliable RPC state has been set to "client commit"

- `USR6306N` - Retrieve the status of all reliable RPC messages of the user who is currently logged on to the EntireX Broker.

For further information, see *Reliable RPC* in the *Natural Remote Procedure Call (RPC)* documentation.

Support of Integrated Authentication Framework (IAF) on Server Side

If Natural Security is installed on the Natural RPC server side and if the EntireX Broker uses IAF for authentication, the Natural RPC server can optionally be configured to use an IAF token for client authentification instead of the Natural Security logon data. The IAF token is provided by the EntireX Broker and contains the user ID that the client has used to log on to the EntireX Broker. As a consequence, after a successful authentication the Natural user ID `*USER` is always identical to the client user ID used by the EntireX Broker. It is no longer possible to use a user ID within Natural that is different from the client user ID used by the Entirex Broker.

To use this feature, the Natural RPC server and IAF must be configured in Natural Security. See the section *Protecting Natural RPC Servers and Services* in the *Natural Security* documentation for details.

No changes are required on the client side.

Note:
The limitations for the Integrated Authentication Framework (IAF) as described for Version 6.3.4 no longer apply.

Natural Security

The following enhancements are provided with Natural Security Version 6.3.5:

- Administrator Services
- Libraries
- DDMs
- Utilities
- Natural RPC Server Profiles
- Other Enhancements

Administrator Services

The following enhancements are provided in Administrator Services:

- Logging of Maintenance Functions
- Maintenance Log Records
- Module Protection Mode
- Definition of Undefined Libraries
- Disable Rename and Delete of Library Node

Logging of Maintenance Functions

The general option **Logging of Maintenance Functions** has been enhanced: When you activate the logging for user and library security profiles, you have the option to log the following additional data (extended logging):

- When the functions Copy User and Copy Library are used with the **with links** option, any relationship which the copying has established between the user/library 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.
- When a link between a group and a library is maintained, a list of the group's members is logged.
- When the Disallow/Allow Modules section of a library (or special link) profile is maintained, information on the changed status of any module is logged.

A new **Log File Maintenance** function, **List Log Records Extended**, is available to view the additional data.

The modifications which are logged for a type of security profiles now also include the transfer of security profiles of this type via the Natural Security data transfer programs SECULD2 and SECLOAD.

Maintenance Log Records

With the **Maintenance Log Records** functions you can display for each log record the screen which was modified. These screens now also show the Natural Security version and the FSEC system file with/on which the modification was performed.

Note:
This 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.

Module Protection Mode

The new option **Module Protection Mode** affects how the **Disallow/Allow Modules** settings in library security profiles are evaluated: You can set it so that they are evaluated in the same way on mainframes and non-mainframe platforms. This may be useful if you transfer a Natural application from a mainframe to a non-mainframe platform and wish to keep your module protection unchanged.

For details, see *Module Protection Mode* under *Library and User Preset Values* in the *Administrator Services* section of the *Natural Security* documentation.

Definition of Undefined Libraries

The new Administrator Services function **Definition of Undefined Libraries** serves the same purpose as the library maintenance enhancement described under *Undefined Libraries* below.

Disable Rename and Delete of Library Node

The new option **Disable Rename and Delete of Library Node** allows you to prevent the inadvertent deletion/renaming of a library in the mapped environment of the Natural Development Server. If it is set, the actions Rename and Delete cannot be selected from the context menu of the library node.

For details, see *Disable Rename and Delete of Library Node* under *Library and User Preset Values* in the *Administrator Services* section of the *Natural Security* documentation.

Libraries

The following enhancements are provided for libraries:

- Source Locking
- Undefined Libraries

Source Locking

Source locking in the case of concurrent updates of Natural source members - as controlled for the Natural session by the Natural profile parameter SLOCK - can now also be controlled for individual libraries by a corresponding setting in the *Session Parameters* section of library profiles.

Undefined Libraries

Library maintenance has been enhanced allowing you to search for undefined libraries - that is, libraries which exist on the system file, but for which no security profiles have been created in Natural Security: You can expand the Library Maintenance selection list to list either all (defined and undefined) libraries or only the undefined ones. You can apply the search for undefined libraries to the current FUSER system file or to another system file of your choice.

For details, see *Listing Undefined Libraries* in the *Library Maintenance* section of the *Natural Security* documentation.

DDMs

The following enhancement is provided for DDMs:

- Support of FDDM Profile Parameter on Non-Mainframes

Support of FDDM Profile Parameter on Non-Mainframes

If a central system file for non-mainframe DDM storage (outside of libraries) is specified with the Natural profile parameter FDDM, the protection of non-mainframe DDMs and the maintenance of their security profiles is performed in the same way as with mainframe DDMs (as described in the section *Protecting DDMs On Mainframes* of the *Natural Security* documentation.

Utilities

The following enhancements are provided for utilities:

- All Utility Profiles
- SYSDDM
- SYSMAIN
- SYSOBJH - Object Handler

All Utility Profiles

In a utility profile, you allow or disallow each option by marking it with "A" or "D" respectively. For ease of maintenance, you can now set all options in a utility profile simultaneously to "A" or "D" by pressing PF16 or PF17 respectively.

SYSDDM

A new `SYSDDM` function **SQL Services (NSB)** for Natural SQL Gateway support is provided with this Natural version. Its use can also be controlled in SYSDDM utility profiles.

SYSMAIN

In the default utility profile of the `SYSMAIN` utility, a new **Additional Option** named **Utilities Option** is available. With it, you can make the **Utilities** option in library profiles apply to `SYSMAIN`.

SYSOBJH - Object Handler

Several new Object Handler functions are provided with this Natural version. Their use can also be controlled in SYSOBJH utility profiles.

Natural RPC Server Profiles

Support of Integrated Authentication Framework

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

See also *Known Issues* above.

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

Note:
The limitations for the Integrated Authentication Framework (IAF) as described for Version 6.3.4 no longer apply.

Other Enhancements

The following other enhancements are provided:

- Selection Criterion for Link Functions
- Control Use of TEST Command in Environments
- Application Programming Interface NSCLI Enhanced
- New User Exit for LOGOFF

Selection Criterion for Link Functions

Whenever you invoke a link function, a window appears before the list of objects to be linked is displayed. This window, which also allows you to specify a start value for the list to be displayed, used to provide an option **Select only defined ones**. This option has been enhanced and is now called **Selection Criterion**: It allows you to select whether the list is to contain:

- all objects (linked and not linked),
- only objects which are already linked,
- only objects which are not yet linked.

This enhancement is provided for all Natural Security maintenance functions available to link users to libraries, users to applications, users to external objects, and libraries to files.

Control Use of TEST Command in Environments

A new option in the security profiles of environments allows you to control the use of the Natural system command `TEST` in an environment. You can allow or disallow it altogether, or restrict the use of the debugger. For details, see *Components of an Environment Profile* in the section *Protecting Environments* of the *Natural Security* documentation.

This option only applies to environments on mainframe computers.

Application Programming Interface NSCLI Enhanced

The application programming interface (API) `NSCLI` has been enhanced: It allows you to list library profiles (and special link profiles) which contain a specific Adabas password, and you can then change the password. For details, see example program `PGMLI006` and text member `TXTLI006` in the library `SYSSEC`.

New User Exit for LOGOFF

A new user exit, `LOGONEX5`, is available; it is invoked by the Natural Security logon program whenever the `LOGOFF` system command is executed.

Documentation

Editors

The documentation for the program editor and for the data area editor has been revised. See *Program Editor* and *Data Area Editor* in the *Editors* documention.

Natural Web I/O Interface

The documentation for the Natural Web I/O Interface has been revised.

An introduction to the Natural Web I/O Interface is now available.

In addition to the information about the new configuration tool, the installation and configuration information for the Natural Web I/O Interface daemon has been moved to the *Natural Web I/O Interface* documentation. This information was previously available in the *Installation* documentation.

The general term "Natural Web I/O Interface server" is now used instead of "Natural Web I/O Interface daemon".