# Common Features of Wrappers and RPC-based Components

This chapter provides additional information on concepts and features common to all wrappers and RPC-based components. It covers the following topics:

- Change RPC Password by Wrappers and RPC Clients
- Natural Logon or Changing the Library Name
- Conversational RPC
- Non-conversational RPC
- Natural Security
- RPC Compression

---

## Change RPC Password by Wrappers and RPC Clients

The application programmer can embed an RPC password change in an application. This is useful if the application programmer wants to provide this functionality to end users of RPC applications. It is necessary if the RPC server forces alteration of the RPC password, otherwise denying use of the RPC server.

The functionality is provided with a special-purpose IDL:

```
Library 'SAGCRPW' : 'SagChangeRPCPassword' is
  Program 'SAGCRPW' : 'changeRPCPassword' is
    Define Data Parameter
              1 newRPCPassword (A8) in
    End-Define
```

The prefix "SAG" is reserved and is used for Software AG delivered IDL files and must not be used by customer applications; see *Rules for Coding Library, Library Alias, Program, Program Alias and Structure Names* under *Software AG IDL File*.

Proceed as follows:

- Define the IDL in the Workbench Editor and generate a wrapper as you would for any other IDL.
- Write a wrapper client program and issue an RPC request as you would for any other IDL. See the documentation on EntireX wrappers for an example.
- Specify the old RPC password in the same way as for any other RPC request issued. See the wrapper documentation on how to specify the password.

### Natural RPC Server running under Natural Security

- may force the user of an application to alter the RPC Password, e.g. in the following situations:
  - NAT838:

    ```
    Change your password. Enter the old and a new password
    ```

  - NAT873:

    ```
    User ID or password invalid
    ```

### Other RPC Servers

- do not support this functionality.

# Natural Logon or Changing the Library Name

The library name sent with the RPC request to the EntireX RPC or the Natural RPC Server is specified in the Software AG IDL file (see `library-definition` under *Software AG IDL Grammar*). The library name can be overridden by wrapper-specific methods, see your wrapper documentation.

For EntireX RPC Servers, depending on the target server, the library name

- is used by an EntireX Java RPC server. The program name is a method within the class called as the name of the class called. See *Administering the EntireX Java RPC Server* under UNIX | Windows.
- is used by an EntireX RPC server under Windows as the name of the dynamic-link library (DLL). The program name is a function export within the DLL called. See *Administering the EntireX Java RPC Server* under UNIX | Windows.
- is used by an EntireX RPC server under UNIX as the name of the shared library or shared object called. The program name is a function export within the shared library or shared object called. See *Administering the EntireX Java RPC Server* under UNIX | Windows.
- is customizable if a CICS RPC Server is used. See *Locating and Calling the Target Server*.
- for *Conversational RPC* is considered for every remote procedure call that belongs to the conversation.

For Natural RPC servers, the library name

- is used as the Natural library name
- can have a maximum length of 8 characters
- is considered only if Natural Logon is forced, even to Natural RPC Server running without Natural Security. If Natural Logon is not given, a Natural RPC Server (under Natural Security or non-security) does not consider the library name. See your EntireX Wrapper documentation for information on how Natural Logon can be forced.

- for *Conversational RPC* is evaluated at the time the conversation is opened. During an ongoing RPC conversation the Natural library cannot be changed due to Natural RPC rules.

# Conversational RPC

EntireX RPC and Natural RPC also supports conversational communication (also known as connection-oriented communication), where the two partners (client and server) retain a communication link over several remote procedure calls.

A context can be maintained on the server side when a Natural RPC Server is in use. See the `DEFINE DATA CONTEXT` statement in the appropriate Natural documentation.

EntireX Wrappers and RPC clients allow termination of an RPC conversation either successfully or abnormally by offering two different methods or function calls for ending an RPC conversation. See the appropriate EntireX Wrapper or RPC client documentation for information on how to initiate the end of an RPC communication.

If communicating with a Natural RPC Server and

- the RPC conversation is ended normally,

  the Natural RPC Server executes a Natural `END TRANSACTION` statement, resulting in a commit of all database manipulations at the server side done within the RPC conversation;

- the RPC conversation is aborted,

  the Natural RPC Server executes a Natural `BACKOUT TRANSACTION` statement, resulting in a backout of all database manipulations done at the server side within the RPC conversation.

See your Natural and Natural RPC documentation for more information.

If communicating with an EntireX RPC Server

- no automatic database processing is initiated. Aborting and closing an RPC conversation are the same and have no effect if database manipulations were done at the server side within the RPC conversation.

# Non-conversational RPC

The basic method of communication for both the EntireX and the Natural RPC is non-conversational (also known as connectionless communication).

Using this method,

- each RPC request is isolated and has no relationship to any other RPC request.
- there is no context and no context could be maintained by the RPC Server.

# Natural Security

A Natural RPC Server may run under Natural Security to protect RPC requests. RPC clients need to be

- **authenticated**
  i.e. the RPC client needs to be defined within Natural Security. Authentication is done with a user ID/password check.
- **authorized**
  i.e. the RPC client needs to be allowed to access programs in the target Natural library, otherwise a security violation error will be returned.

See your Natural Security documentation for more information.

# RPC Compression

RPC compression is a feature used to reduce network data sizes. EntireX tries to select RPC compression automatically. If RPC compression is supported by your RPC server, we recommend using it.

## Natural RPC Servers

Natural RPC Servers running under Natural version 3.1.6 and later support RPC compression. If you are communicating with Natural RPC version 5.1.1 and later, RPC compression is selected automatically. To enable connection to earlier versions of Natural RPC Servers, EntireX wrappers and RPC technology allow you to switch off RPC compression.

## EntireX RPC Servers

All versions of the EntireX RPC server support RPC compression. If you are communicating with an RPC server using EntireX 5.3.1 and later, RPC compression is selected automatically.