

domibusConnector-4.1.0-RELEASE - InstallationGuide

Table of contents

TABLE OF CONTENTS	2
1. INTRODUCTION	4
1.1. SCOPE AND OBJECTIVE OF THIS DOCUMENT	4
1.2. THE DOMIBUSCONNECTOR AS A WEB APPLICATION	4
1.3. THE DOMIBUSCONNECTORCLIENT	4
1.4. THE GATEWAY	4
1.5. THE DOMIBUS-CONNECTOR-PLUGIN	5
2. PRECONDITIONS AND TECHNICAL REQUIREMENTS.....	6
2.1. SUPPORTED OPERATING SYSTEMS	6
2.2. JAVA RUNTIME	6
2.3. DATABASE	6
2.4. WEB CONTAINER	6
2.5. INTERNET CONNECTION.....	7
2.6. TECHNICAL SPECIFICATIONS	7
2.7. THE DOMIBUSCONNECTOR DISTRIBUTION PACKAGE	7
3. DATABASE INSTALLATION.....	9
3.1. SUPPORTED DATABASE VENDORS	9
3.2. NEW DATABASE / FRESH INSTALLATION.....	9
3.2.1. USING THE SCRIPTS.....	9
3.2.2. USING LIQUIBASE	9
3.3. DATABASE UPGRADE 3.5 TO 4.1.0.....	9
3.3.1. USING THE SCRIPT	10
3.3.2. USING LIQUIBASE	10
3.4. UPGRADE WITH LIQUIBASE	10
4. CERTIFICATE, KEY-STORES AND TRUSTSTORES.....	12
5. CONFIGURATION PROPERTIES	13
6. DEPLOYMENT.....	14
6.1. DEPLOY ON APACHE TOMCAT	14
6.1.1. TESTED TOMCAT VERSION	14
6.1.2. DEPLOYMENT STEPS	14
6.2. DEPLOY ON BEA WEBLOGIC	14
7. THE DOMIBUSCONNECTOR ADMINISTRATION UI	15
8. IMPORT OF P-MODES	16
8.1. IMPORT OF A P-MODE FILE WITH THE DOMIBUSCONNECTOR ADMINISTRATION UI	16
9. BACKEND CONFIGURATION	17
9.1. BACKEND TYPES.....	17

9.1.1.	PUSH/PULL BACKEND.....	17
9.1.2.	PUSH/PUSH BACKEND.....	17
9.2.	ADDING THE BACKEND CLIENT KEYS TO THE CONNECTOR BACKEND KEY STORE.....	17
9.3.	CONFIGURING THE BACKEND WITH THE DOMIBUSCONNECTOR ADMINISTRATION UI	18
9.4.	CONFIGURING THE BACKEND AT THE DATABASE.....	18
9.4.1.	DOMIBUS_CONNECTOR_BACKEND_INFO	19
9.4.2.	DOMIBUS_CONNECTOR_BACK_2_S.....	19
9.4.3.	EXAMPLE SCRIPTS.....	19

1. Introduction

1.1. Scope and Objective of this document

This document is a technical guide to install and configure the domibusConnector 4.1.0-RELEASE. It can be used as a “go-through” installation guide. Readers should be able to install and configure the domibusConnector in their own environments without previously built know-how about the software.

The target audience of this document are technical personal or administrators that have experience in network environments and widely known software components like web servers or application servers.

A detailed knowledge of the own network structures and environment is a precondition.

The structure of this guide is built so that every step can be taken as listed in the document. That means all preconditions for a chapter should be given by the previous chapters.

As an InstallationGuide this document does not focus on features and functionalities on the usage of the domibusConnector. For more details on the usage please read the “domibusConnector_Technical-documentation-and-UserGuide” distributed together with the domibusConnector-4.0-RELEASE.

1.2. The domibusConnector as a web application

Starting with version 4.0-RELEASE, the domibusConnector is on the technical basis of a web application.

This means, that the domibusConnector itself is a “ready-to-use” software component that only needs to be configured, set-up and deployed in a web container.

Once installed and configured properly, the domibusConnector should run on its own.

1.3. The domibusConnectorClient

The domibusConnector web application offers different interfaces that can be used to approach the functionalities. Those interfaces can be used directly, if intended.

To close the missing link between your own implementation and the provided web service of the domibusConnector, a domibusConnectorClient was implemented to support the connection to the domibusConnector.

The domibusConnectorClients and all its variants and usage are described in the document “domibusConnectorClient_Guide”.

1.4. The gateway

To establish a successful connection to e-CODEX network partners, it is necessary to have a gateway component for transmission of messages.

To be able to connect with e-CODEX partners the ebms3 standard of OASIS must be respected by the gateway. Additionally, there are different profiles on how the structure of ebms3 messages can be transmitted. In e-CODEX all partners agreed on using the e-SENS-AS4 pattern.

During the e-CODEX project an own gateway component was implemented as a building block that fulfils all mentioned requirements. This is the DOMIBUS Gateway.

Today the development and maintenance of the DOMIBUS Gateway lies at the CEF program of the European Commission.

Further details on the DOMIBUS gateway can be found at the CEF homepage:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus>

1.5. The domibus-connector-plugin

To have a connection between the domibusConnector and the Domibus Gateway, a plugin has been developed that can easily be installed on the gateway.

This plugin implements all interfaces that enable message transmission between the connector and the gateway. It is also available as a distribution package of e-CODEX on the Nexus repository server:

<https://secure.e-codex.eu/nexus/content/groups/public/eu/domibus/connector/domibus-connector-plugin/>

Details on how to install the plugin on the Domibus Gateway can be found in the documentation of the respective Domibus Gateway and as an Installation-Guide with the domibus-connector-plugin distribution.

2. Preconditions and technical requirements

This chapter describes what has to be in place prior to install the domibusConnector. It also lists some technical specifications of the domibusConnector to give a more detailed insight.

2.1. Supported operating systems

The domibusConnector is a software that has been completely implemented using the JAVA programming language.

As JAVA is by definition a platform independent environment, every operating system with a proper JAVA installation should fit the needs of setting up the domibusConnector.

During implementation and testing phase of the domibusConnector, it was installed and tested on the following environments:

- Microsoft Windows 7
- Linux
- IBM AIX

2.2. Java Runtime

As the domibusConnector is a JAVA application, it also requires a proper installation of a Java Runtime to be able to run the software.

The recent version 4.1.0-RELEASE of the domibusConnector has been implemented and compiled with an Oracle JDK jdk-8u161. So at least this version or higher should be in place to avoid incompatibilities.

2.3. Database

The domibusConnector needs an underlying database to store information. Currently the following DBMS are supported:

- MySQL 5.5 and higher
- Oracle 12g and higher

The domibusConnector distribution package offers SQL scripts that are meant to either set up a completely new database for the connector, or to migrate an existing domibusConnector database to its current version.

Be aware that most web-servers need to have proper JDBC drivers installed to be able to set the connection to the database.

Details on the installation of the database can be found in the chapter [Database Installation](#).

2.4. Web container

Since the domibusConnector in its current version 4.1.0-RELEASE is a web application built as a WAR deployable, it needs a web-server or application server that it can be deployed at.

This can be any JAVA compliant product which supports at least Servlet 3.0 API level.

During implementation and testing of the domibusConnector the following web-servers were used:

- Apache Tomcat 8
- Oracle Bea WebLogic 12c

Be aware that those are neither requirements nor recommendations, but only listed for information. This installation guide does not focus on specifics of web-server technologies in detail. Details on how to deploy the domibusConnector on that web server products can be found in chapter [Deployment](#).

2.5. Internet connection

As the domibusConnector needs some sources from the internet for the security library features, also an internet connection from the installation point must be given. To be able to configure your environment the domibusConnector gives the opportunity to configure proxy settings in the connector properties described in chapter [Configuration properties](#).

2.6. Technical specifications

The main frameworks and technologies the domibusConnector was implemented with is listed here for your information:

- Java 8 (Oracle jdk-8u161)
- Spring framework 5.0.8.RELEASE
- Spring-boot 2.0.4.RELEASE
- Hibernate 5.0.12.FINAL
- Apache CXF 3.2.1
- Apache Maven 3

2.7. The domibusConnector distribution package

To get started, you first need to have downloaded and extracted the distribution package.

The domibusConnector provides different distribution packages all placed on the e-CODEX Nexus repository server at:

<https://secure.e-codex.eu/nexus/content/groups/public/eu/domibus/connector/domibusConnectorDistribution/4.1.0-RELEASE/>

- domibusConnectorDistribution-4.1.0-RELEASE.zip

Once downloaded and extracted it has the following structure:

File/directory	Description
Webapp (directory)	This directory contains the application itself distributed as "domibusConnector-4.1.0-RELEASE.war"
Documentation/database-scripts (directory)	This directory contains all necessary database scripts to set up the database for the domibusConnector. The scripts are prepared for the database vendors MySQL and Oracle. For more details see chapter Database Installation

Documentation/databaseInitializer (directory)	Contains the “domibusConnectorDatabaseInitializer.jar” which is a helper application to set up the database. For more details see chapter Database Installation
Documentation/properties (directory)	The “properties” folder contains example properties that show how to configure the domibusConnector. The log4j configuration is also contained as an example.
domibusConnector_Monitoring_Interfaces.pdf	A document that describes what monitoring interfaces the domibusConnector offers and how to approach them.
domibusConnector-Technical-documentation-and-UserGuide.pdf	This document merges the documentation for the domibusConnector for administrators and users. This document covers all distributions of the domibusConnector.

3. Database Installation

The “domibusConnectorDistribution-4.1.0-RELEASE.zip” deliverable package contains database scripts to either create a new database or upgrade an existing database for domibusConnector 3.5(.1) to domibusConnector-4.0 to 4.1.0.

As a precondition a DBMS already needs to be in place. We recommend to create an own schema/user for the domibusConnector database.

3.1. Supported Database vendors

Tests for the domibusConnexor have been done using the following databases:

- Mysql from version 5.5 onwards
- Oracle from version 12g onwards

Prepared database scripts exist only for those vendors. Though, any other SQL database can be used.

3.2. New Database / Fresh Installation

Starting with a new installation and therefore have an empty schema/user on the database system created, one has just to execute the provided scripts or use liquibase.

3.2.1. Using the scripts

The documentation contains a folder database-scripts/initial. This folder contains the following DDL/SQL scripts:

- “MySql_4_1_initial.sql” for MySQL
- “Oracle_4_1_initial.sql” for Oracle

Once those scripts are executed on the dedicated schema, the database is ready for usage for the domibusConnector.

3.2.2. Using liquibase

It is also possible to let liquibase create your database tables. Start reading the section “Upgrade with Liquibase” down below.

3.3. Database Upgrade 3.5 to 4.1.0

Upgrading an existing domibusConnector database for prior releases 3.5 or 3.5.1 is possible. But first of all we strongly recommend to create a backup of the existing database schema.

Then you can choose to upgrade your database schema manually by executing the scripts or let liquibase do the work.

Both methods are assuming that there are no changes or additional constraints, indexes added

compared to the 3.5 database script.

3.3.1. Using the script

- Create a backup of your current database schema
- Drop/deactivate all foreign-key constraints (the script will create them again!)
- Execute the upgrade script which is located in the folder database-scripts/migration.

Use the script for your database vendor:

- “MySQL_Migrate_3.5_ConnectorDB_to_4.0.sql” for MySQL
- “Oracle_Migrate_3.5_ConnectorDB_to_4_0.sql” for Oracle
- Repeat the same with the “*Migrate_4.0_ConnectorDB_to_4.1.sql”

3.3.2. Using liquibase

If you want to use liquibase for database upgrade please continue with the next section “Upgrade with Liquibase”.

3.4. Upgrade with Liquibase

It is also possible to let liquibase upgrade or create your database. Liquibase is a tool which splits the database creation/upgrade into multiple changesets. In the future it will allow semi automatic database upgrades. You can also use liquibase to use unsupported databases like postgresql.

Liquibase is packaged into the jar named domibusConnectorDatabaseInitializer.jar which includes all the necessary database scripts:

- Database Migrate 3.5 to 4.0 DB ChangeLog: “db/changelog/v004/upgrade-3to4.xml”
- Database Create 4.1 DB ChangeLog: “db/changelog/install/initial-4.1.xml”

You can execute the scripts in your database by executing the jar:

```
java -jar domibusConnectorDatabaseInitializer.jar --changeLogFile=${changeLogFile} \
--driver=${sqlDriverName} \
--url=${databaseUrl} \
--username=${databaseUsername} \
--password=${databasePassword} \
--classpath=${jdbcDriverJar} \
upgrade
```

You have to provide the following parameters:

- “--driver=” the jdbc driver name.
 - com.mysql.jdbc.Driver for MySQL
 - oracle.jdbc.OracleDriver for Oracle
- “--url=” the jdbc url to access the database (consult the documentation of your jdbc driver)
 - Example: “jdbc: mysql://localhost/domibusconnector” for connecting to a local MySql database named domibusconnector.

- “--username=” the username to access the database. The database user needs the permission to make schema modifications.
- “--password=” the password of the database user.
- “--classpath=” the path to an additional jar which contains the jdbc driver (the package already contains the mysql jdbc driver, so this parameter is only needed to provide the oracle jdbc driver jar)
- “--changeLogFile=” the change log liquibase should run against the database
- “--help” will show the liquibase help

4. Certificate, Key-Stores and Truststores

To ensure the highest reasonable level of security, the domibusConnector uses several certificates for different purposes:

- Signing and Encrypting SOAP messages between the backend client and the Connector.
- Establishing Transport Security (TLS) between the backend client and the Connector.
- Signing and Encrypting SOAP messages between the Connector and the Gateway.
- Establishing Transport Security (TLS) between the Connector and the Gateway.
- Validating the signature of the main document (mostly a PDF) of the message (if configured).
- Validating the signature of the secure container (ASIC-S) received with incoming messages.
- Signing the secure container (ASIC-S) that is created by the Connector.
- Signing the ETSI-REM evidences.

In most of those cases the same certificate can be used, though we do not recommend that. For higher security it is more efficient to use different certificates.

The keys and stores, for the backend client(s) for example, are explained in more detail in the document “e-Codex_key_trust_stores.pdf”.

5. Configuration properties

In order to give the domibusConnector the missing links about your environment, some properties have to be set in a property file. Usually this is called “connector.properties”.

There is also the possibility to adopt the logging configuration. This gives the opportunity to control where logs are written to and what to log.

Example properties and an empty property file, as well as an example for logging configuration can be found in the distribution package at “documentation/properties”.

The properties in those file are all well described on what is expected there.

The connector properties must be given as an environment variable with name “connector.config.file” on the web server.

The logging configuration must be given as an environment variable with name “connector.logging.config” on the web server.

The variants on how to set those environment variables on your web server environment is dependent on what product you have in place.

For the web server products Apache Tomcat and BEA Weblogic this is described exemplarily in the Chapter [Deployment](#).

6. Deployment

This chapter describes the steps to be taken to deploy the domibusConnector application on a web server. The e-CODEX community can provide more detailed information for the web server products Apache Tomcat and BEA Weblogic. Other Web Servers have not been subject to any tests.

It is not a requirement that one of the listed web server products must be used.

6.1. Deploy on Apache Tomcat

6.1.1. Tested Tomcat Version

The deployment has been tested with the following versions:

- Apache Tomcat 8.5.23 on Windows 7

6.1.2. Deployment steps

- Copy the adopted “connector.properties” and “log4j.properties” file into “<path_to_tomcat>/conf/domibusConnector”.
- Copy the “domibusConnector.war” into “<path_to_tomcat>/webapps”.
- Create or edit a “setenv” file at “<path_to_tomcat>/bin”.
- Optionally copy your database driver JAR into “<path_to_tomcat>/lib”.

The “setenv” file should be called at startup by the tomcat and should include the following parameters:

```
REM   Please change CATALINA_HOME to the right folder (below line only works if you start from current folder)
REM   set CATALINA_HOME=<YOUR_INSTALLATION_PATH>

set JAVA_HOME="C:\Entwicklung\jdk1.8.0_121"
set JRE_HOME="C:\Entwicklung\jdk1.8.0_121\jre"
set JAVA_OPTS=%JAVA_OPTS% -Dconnector.config.file=%CATALINA_HOME%/conf/connector/connector.properties
set JAVA_OPTS=%JAVA_OPTS% -Dconnector.logging.config=%CATALINA_HOME%/conf/connector/log4j.properties
```

Finally start/restart your Apache Tomcat. The application should be deployed automatically.

6.2. Deploy on BEA Weblogic

The connector application is a spring boot application which should run on a weblogic application server.

In its default configuration it expects a jndi DataSource configured with the name

“domibusWebConnectorDS”. Please configure a datasource with this name and deploy the application

to your weblogic server. You should also set the “connector.config.file” parameter to your “connector.properties” so the spring boot application can load the configured settings.

For that purpose you need to create a custom deployment descriptor.

7. The domibusConnector Administration UI

Once the domibusConnector is successfully deployed in a web container and running, the pages of the domibusConnector – the domibusConnector Administration UI - can be reached at

<http://<yourServer>:<configuredPort>/domibusConnector/admin/>.

Username

Password

The default login already stored in the database for the web user interface is “admin” with the password “admin”. As this is a very unsecure authentication, the “admin” password is automatically expired and needs to be changed for the first login.

The following chapters only describe the installation parts necessary to run the domibusConnector. Other functionalities of the domibusConnector Administration UI are described in the “domibusConnector-Technical-documentation-and-UserGuide.pdf” distributed with the domibusConnector package.

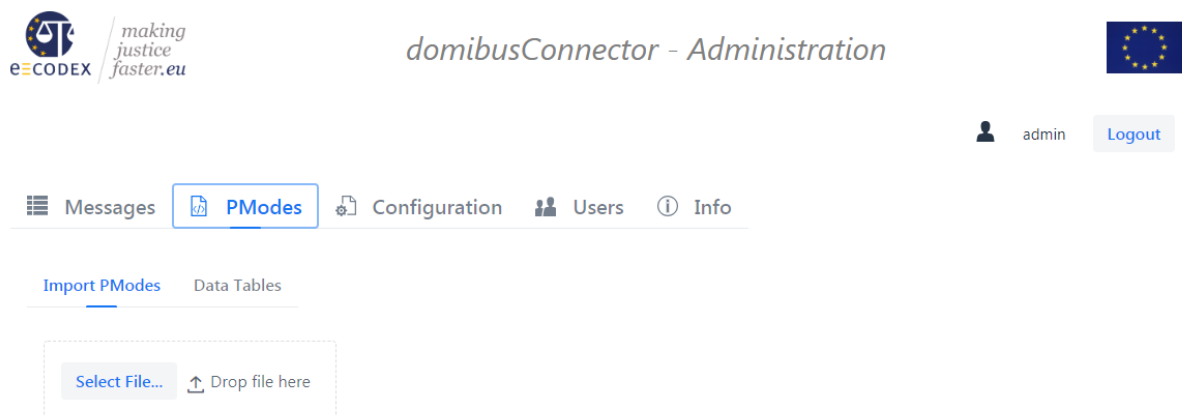
8. Import of p-modes

The “p-modes” that are distributed by the configuration management for the DOMIBUS gateway can also be used for the domibusConnector database to have necessary data to support business use cases in your domibusConnector database.

If the installed domibusConnector is not a completely new one but a migrated one from a previous version, this step should not be necessary.

8.1. Import of a p-mode file with the domibusConnector Administration UI

Once logged in at the Administration UI, the requested functionality is reachable via menu option “PModes”.



The p-mode file from the configuration management can be selected here and will be uploaded into the database of the domibusConnector.

Every ACTION, PARTY and SERVICE that is found in the p-modes and which do not exist in the database already, will be created. The domibusConnector will neither change any existing database items (service, action or party), nor will it delete any of those. If the p-mode-file cannot be processed an error message will appear.

9. Backend configuration

The domibusConnector can be accessed by multiple clients. It does not matter, if the clients use the distributed domibusConnectorClient (either one of the libraries for integration, or the standalone client), as long as the backend interfaces of the domibusConnector are implemented properly and the security needs can be met.

This guide focuses on the configuration needed to add new backend clients to connect to the domibusConnector. Details on configuration steps needed on the client side can be found in the domibusConnectorClient documentation.

This chapter follows an example in which 2 new backend clients should be configured in the domibusConnector:

- Alice
- Bob

9.1. Backend types

Whereas it is given in version 4.1.0-RELEASE of the domibusConnector that the backend interfaces only can be reached via SOAP web services, it can be configured if the backend client supports to be called as an active service.

9.1.1. Push/pull backend

This type of backend client does not support an active web service itself. It can only be seen as a passive client. The domibusConnector can receive messages from this type of client at any time, but cannot actively send messages to the client.

That means that the client itself has to call the web service of the domibusConnector to receive messages that are stored inside the connector until the client calls them.

Mostly this is done by having time triggered jobs running on the client side that connector to the domibusConnector to receive its messages.

The domibusConnectorClient Standalone variant is of that kind.

9.1.2. Push/push backend

This type of backend client does support an active web service. This web service must run in a web container itself and must implement the delivery web service of the domibusConnector. In that case the domibusConnector does not need to wait until the clients connects, but can push messages to the client by itself.

9.2. Adding the backend client keys to the Connector Backend Key Store

Every new backend client needs its own certificate.

The certificate of a backend client has the following purpose:

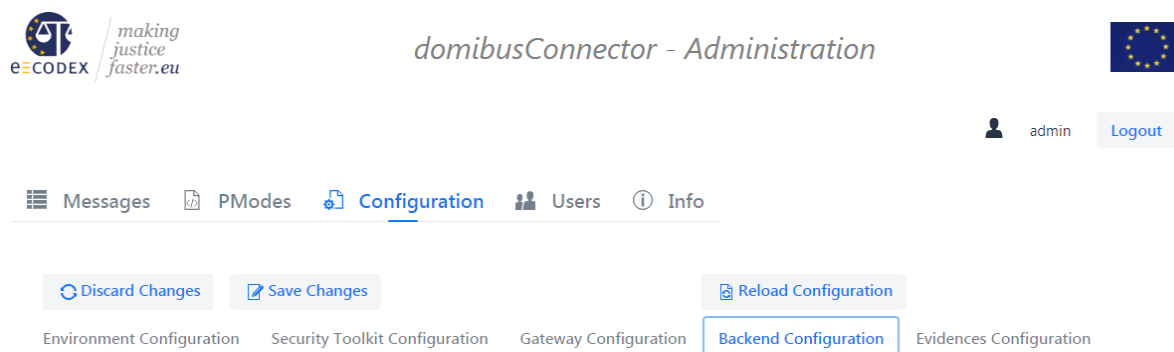
- Identifies the backend client when it connects to the domibusConnector
- Encrypts/Decrypts messages between the backend client and the Connector.

So let's assume, following the example of "alice" and "bob", that there are 2 certificates. What we need to configure the backend clients properly, are the public keys of those certificates.

Those 2 public keys need to be added to the "Connector Key Store" described and configured in chapter 5.1. To keep it transparent the public keys are imported into the store with the alias names "alice" and "bob".

9.3. Configuring the backend with the domibusConnector Administration UI

Within the Administration UI, go to menu "Configuration" and further on "Backend Configuration"



domibusConnector - Administration

admin Logout

Messages PModes **Configuration** Users Info

Discard Changes Save Changes Reload Configuration

Environment Configuration Security Toolkit Configuration Gateway Configuration **Backend Configuration** Evidences Configuration

Details	Backend Name	Key Alias	Default	Push Mode	Enabled	Push Address
	connector-client	connector-client	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

On this page, the section "Configured Backend(s)" is of interest for this step

Configured backend(s):

[+ Add new Backend Client Info](#)

Details	Backend Name	Key Alias	Default	Push Mode	Enabled	Push Address
	connector-client	connector-client	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

9.4. Configuring the backend at the database

For the domibusConnector-4.1.0-RELEASE the adding of the backend must be done manually by accessing the domibusConnector database. The backend information must be stored in two database tables:

9.4.1. DOMIBUS_CONNECTOR_BACKEND_INFO

Name	Description
ID	a unique technical id
BACKEND_NAME	The name of the backend this name must match the common name (CN) field of the assigned certificate
BACKEND_KEY_ALIAS	The key alias in the connector backend keystore for the certificate to use to encrypt messages for the connectorClient
BACKEND_KEY_PASS	If the key is encrypted this column contains the password
BACKEND_SERVICE_TYPE	Not used yet, will later define the type of the backend, is it push/pull, push/push over webservises, push/push over jms
BACKEND_ENABLED	Is the backend enabled, must be true if the connector should send messages to this backend
BACKEND_DEFAULT	The default backend will receive all messages which aren't delivered to another backend first
BACKEND_DESCRIPTION	A description of the backend, can be used by the admin to store information
BACKEND_PUSH_ADDRESS	If the backend is a push backend, push address must be defined here

9.4.2. DOMIBUS_CONNECTOR_BACK_2_S

Contains the routing information, which backend will receive the message. The routing decision is based on the name of the business use case, which is called SERVICE in e-CODEX.

The table contains the following fields:

DOMIBUS_CONNECTOR_SERVICE_ID	References the service
DOMIBUS_CONNECTOR_BACKEND_ID	References the backend

9.4.3. Example scripts

Now we will have a look back to our example, where we want to add “alice” and “bob” as our new backend clients.

The following SQL statement will add an connectorClient named bob with the key alias bob and expects that the common name of the certificate is bob. Bob will also be the default backend!

```
INSERT INTO domibus_connector_backend_info
(ID, BACKEND_NAME, BACKEND_KEY_ALIAS, BACKEND_ENABLED, BACKEND_DEFAULT)
VALUES ('11', 'bob', 'bob', TRUE, TRUE);
```

The following statement will add “alice” to the backend configuration:

```
INSERT INTO domibus_connector_backend_info  
(ID, BACKEND_NAME, BACKEND_KEY_ALIAS, BACKEND_ENABLED, BACKEND_DEFAULT)  
VALUES ('12', 'alice', 'alice', TRUE, FALSE);
```

This statement will assign the epo messages to the connectorClient with the id 12 in the database. In this case this will be the connectorClient alice.

```
INSERT INTO domibus_connector_back_2_s  
(DOMIBUS_CONNECTOR_SERVICE_ID, DOMIBUS_CONNECTOR_BACKEND_ID)  
VALUES ('EPO', '12');
```

