auto-gration Connector
Setup Manual
Installation and configuration of the auto-gration Connector for SMEs
Auto-gration project team

October 2012
This document explains how to obtain and setup the reference implementation of the auto-gration Connector for SMEs.

The software has been developed under the COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL), an open source license and can be used free of charge by any user or software developer.
Contents
Preparation ......................................................................................................................................... 5
Download the software ...................................................................................................................... 6
Extract the content of the Zip file ....................................................................................................... 6
Run the setup ...................................................................................................................................... 7
    Meaning and purpose of the data folders ....................................................................................12
Configure the Connector................................................................................................................... 13
    Run the configuration ................................................................................................................... 13
    Setup the outbound connection(s) ............................................................................................... 14
    Test the outbound connection ..................................................................................................... 16
    Set the message routing table ...................................................................................................... 16
Workflows and User Setup ............................................................................................................... 18
    User management......................................................................................................................... 18
    Setup User actions ....................................................................................................................... 19
    Setup User notifications ................................................................................................................ 20
Create a connection for manual download/upload of messages ..................................................... 22
    Setup the outbound connection(s) ............................................................................................... 22
    Test the outbound connection ..................................................................................................... 23
    Set the message routing table ...................................................................................................... 23
Using the Connector as a Server ....................................................................................................... 24
    Setup an HTTP inbound connection ............................................................................................ 24
    Setup an HTTPS inbound connection .......................................................................................... 25
    Activate the forwarding mode ...................................................................................................... 27
Internal configuration of the Connector ........................................................................................... 28
    Major software artefacts .............................................................................................................. 28
    The csc-hibernate.properties file ............................................................................................... 28
    The csc-settings.properties file .................................................................................................. 30
    Internationalization support ....................................................................................................... 31
    Notification templates ................................................................................................................. 31
    Customize the Archiving function ............................................................................................... 32
Updating the connector with a new version (Windows) .................................................................. 33
    Preparation ................................................................................................................................... 33
    Conducting the update .................................................................................................................. 33
Post-processing ............................................................................................................................. 33
Updating the connector with a new version (linux) ................................................................. 34
Preparation ................................................................................................................................... 34
Conducting the update ................................................................................................................. 34
Post-processing ............................................................................................................................. 34
Preparation

Before you start to install and to deploy the auto-gration Connector there are some requirements to be considered:

**Hardware:**

- X86 Processor;
- Min. 512 MB RAM;
- 10 GB or more disk capacity.

**Operating System and Network Infrastructure:**

- Supported operating systems:
  - Windows XP, Vista or Windows 7 32 or 64 Bit;
  - Linux 32 or 64 Bit;
- Internet access from the computer that runs the Connector: DSL or ADSL is sufficient, no requirement for a fixed IP address or qualified domain name. By default, the Connector uses two ports:
  - One HTTP port for the communication with the user interface, typically the port 8080. However, any other available port can be used instead. This port can also be used for unsecured data exchange with remote stations (Connectors), this should only be done for initial testing purposes or in otherwise secured network infrastructures (such as VPN or intranet);
  - One HTTPS port for secure data transmission (typically 443 or 8443);

These ports must be open on the computer which hosts the Connector in order to allow the Connector to communicate with external partners and also to access the user interface of the Connector. If a proxy is used to separate the intranet from the public Internet, the address and port of the proxy must be known for the setup as well;

- Shared folders for the Connector and local ERP system so that they can exchange files by saving and retrieving them on shared folders.

If you intend to use the Connector as a server (for instance, if you operate a B2B platform and the Connector is intended to react to incoming calls from client Connectors which are installed in your business partners’ systems) you must also have a fixed IP address or domain host name (e.g. www.mycompany.com) so that client Connectors can access the server through the public Internet.

Also, in order to facilitate the HTTPS protocol, you need a server certificate of a trusted issuing Certificate Authority (CA) that confirms your IP address or domain host name. By default, the Odette CA is installed as trusted CA in all Connector clients.

For further details, see also chapter „Using the Connector as a Server“.
Download the software
You can download the software from the auto-gration web-site:
http://www.auto-gration.eu/downloads/software

Select the appropriate package (Win32 or Linux32) and save a copy of the Zip file on your computer.

Extract the content of the Zip file
You can extract the content into any suitable directory.

Please note that you should have write access rights to that directory in order to extract the Zip file.
Run the setup

A double-click on the setup.bat file will start the setup process for Windows. For Linux use instead the setup.sh file (for Linux, you may have to set the „executable“ mode on all the setup.sh and all *.sh files in the tomcat*/bin folder).

Click SETUP.
You must accept the License Agreement by clicking ‘I AGREE’.

Specify **HTTP port**: the selected port is used to connect your computer to the Connector’s graphical user interface (GUI), 8080 is the recommended default.

Specify **Station ID**: each auto-gration Connector is identified by a unique Station ID. You can obtain this ID through the auto-gration web-site (see next picture):

http://www.auto-gration.eu/repository/car-sme-connector-csc-id-registration-request

The ID is generated as a URN (Uniform Resource Name) using the auto-gration namespace, followed by the country code, the company (short) name, the geographical location (e.g. city) and an index. The index is used to distinguish between different stations that a company might have in the same geographical location (e.g. a chain of repair shops).
The station ID request shown in Figure 7 would result in the assignment of the following ID:
urn:autogration:gb:odette:london:001

**Proxy Server Address and Proxy Port Number**: if your company uses an internet proxy, you must specify the server address (usually an IP number like 192.168.1.123) and the port number used to connect to the proxy. If in doubt, contact your network administrator.

**Specify HTTPS port**: the selected port is used by the Connector to accept secured data exchange initiated by remote stations (Connectors). The value 8443 is the recommended default for Windows (use 843 for Linux systems).

![Figure 7](image1.png)

Click NEXT to apply the necessary settings to your Connector.
After the configuration has finished, you must run two additional script files to install the auto-gration service and to start it. Once installed and started, the auto-gration service will automatically run in the background and will also be re-launched automatically whenever you restart the computer hosting the service.

On Windows Vista and Windows 7, run the files install-service.bat and start-service.bat as administrator (on Windows XP you don’t need to run it as administrator).
On a Linux operating system, run the files install-daemon.sh and start-daemon.sh.

The setup creates a data folder under the folder where you are installing the software.

![Figure 11](image.png)
Meaning and purpose of the data folders

The directory where the auto-gration Connector is deployed contains the following sub-directories:

- **archive**: default place where incoming and outgoing messages are archived
- **db**: holds the SQL database that stores all incoming and outgoing messages
- **inbound-to-do-list-folder**: stores inbound messages waiting for user action
- **messages-not-sent-to-internet**: holds messages that could not be sent to the specified destination after the specified number of communication retries.
- **messages-received-from-internet**: holds inbound messages waiting for pick-up by the local ERP system
- **messages-to-send-to-internet**: holds messages generated by the local ERP system and waiting to be picked-up and sent by the Connector
- **outbound-to-do-list-folder**: stores outbound messages waiting for user action
- **request and responses folders**: have the same function as the corresponding message folders, except they are used for request-response transactions (AvailabilityRequest and AvailabilityResponse)
- **proprietary-messages-to-send-to-internet**: holds messages generated by the local ERP system in its proprietary format and waiting to be picked-up, transformed and sent by the Connector
- **proprietary-messages-received-from-internet**: holds inbound messages waiting for pick-up by the local ERP system (messages are in the ERP proprietary format)
- **messages-received-from-internet-and-ignored**: holds inbound messages that could not be transformed to the ERP proprietary format.

Important note:

At the same level as the data folder is a folder for the Tomcat web-server, e.g.

```
...\auto-gration-connector-win32\data
```

```
...\auto-gration-connector-win32\tomcat-7.0.27
```

For security reasons it is strongly recommended that this tomcat-7.x.xx folder can be accessed by the administrator only. Any unauthorised access can compromise the security and the correct functioning of the Connector.
Configure the Connector

The following instructions are based on the assumption that your local Connector acts only as a client and the remote Connector acts as the server (this remote Connector will in most cases be running within a service provider). In this case, you need neither a fixed internet IP address nor a qualified domain hostname (e.g. www.mycompany.com). There is also no requirement for a separate security certificate on your side – the certificate installed on the server of your service provider suffices to ensure a secure data transmission.

Run the configuration

After installation you are able to access the Connector through its user interface and to complete the necessary settings.

If you are logged on to the computer hosting the Connector, you will access the Connector through the following link on your internet browser: http://localhost:8080/autogration where 8080 is the port number you have specified during setup (see Figure 6).

If the Connector is running on a different computer, you can access it through your internet browser using the IP address or domain host name of the computer hosting the Connector followed by the port number and the string ‘/autogration’, e.g. http://192.168.1.10:8080/autogration or http://edi.mycompany.com:8080/autogration. If necessary, contact your network administrator.

Figure 12

Log on to the Connector using the administrator account admin, the default password is also admin.
Setup the outbound connection(s)
Select CONNECTIONS/Outbound Connections.

If you have received the software from your service provider, the necessary settings might be already there¹. If you start from scratch, add a new outbound connection (this will identify the remote Connector to which your Connector is to be linked):

![Outbound Connection](image)

Figure 13

¹ If you downloaded the Connector through the auto-gration web site, your Connector has already an outbound connection in place. This outbound connection links your Connector to a remote Connector running at the computer co-operate.inescporto.pt and allows you to establish communication with that Connector, for testing purposes (after having obtained a Station ID for your Connector, you should have received by email a password for your Connector so that communications can be established with that remote Connector.)
Station ID: Enter the station ID of your remote partner / service provider (e.g. the station ID of the remote Connector).

RemoteHostName: The IP address or domain host name of the remote server, i.e. something like 192.168.1.10 or edi.myserviceprovider.com.

TransportProtocol: The communication protocol to be used to communicate with the remote server (HTTPS is strongly advised, but HTTP is also supported).

RemotePortNumber: The port used by the transport protocol identified above. For HTTPS communication either 443 or 8443 are recommended. For HTTP communication, 8080 is recommended.

RemoteServiceName: The path to the service running on the remote computer.

Password: The password assigned by the remote partner to your account.

Maximum Retries: The maximum number of retries to establish a connection to the remote computer in case the first connection attempt fails.

RetryInterval: The initial interval in minutes between the first and second attempt to connect.

ScalingFactor: The increase of the retry interval between each attempt. The given example would cause an initial interval of 20 minutes, then 30, 45, 67.5, etc.

Set Test Indicator: If ticked, all interchanges are marked as test. Use this for the initial test / setup period and unselect the indicator once you change to operational mode.

Enable Dispatch ...: This will cause messages to be sent immediately to the remote Connector once it is placed in the outbound folder.

Enable Periodic ...: Will cause the Connector to fetch from the server (remote connector), at regular intervals (60 seconds by default), new messages available for download.

Folder for Downloaded ...: Enter the export folder if you are creating an outbound connection for manual upload / download of messages (see section “Create a connection for manual download/upload of messages”).

Save your settings.

If you need to connect to several remote partners (each one having a separate remote Connector), repeat the process for these other partners. As a result you should see the specified outbound connections in the list (Figure 14).
Test the outbound connection
Select CONNECTIONS / Check Connections and click the Check Connection button to test the access to all the outbound connections (see Figure 15).

If the setup is correct, you will see an OK under REMOTE HOST CONNECTION and REMOTE SERVICE.

OK under REMOTE HOST CONNECTION indicates can access the internet and could resolve the Remote Host name. OK under that your Connector REMOTE SERVICE indicates that the service on the remote computer (remote Connector) could be contacted. If there is an error in the REMOTE SERVICE column, there are several possible reasons:

- You entered a wrong path for the service
- You entered a wrong password for your own account
- You specified the wrong port number
- Your own proxy settings are incorrect
- The service at your partner’s site is not running

Please check with your business partner or your network administrator in this case.

If auto-gration messages are not to be sent to a remote Connector but should instead be uploaded to a portal manually an appropriate outbound connection should be specified (see chapter “Create a connection for manual download/upload of messages later in this document”).

Set the message routing table
In order to send the messages to the correct recipients (i.e. remote Connectors), a routing table is used. According to the entries in this table the Connector will select the remote target Connector based on the combination of BuyerID and SellerID (i.e. customer number and supplier number). If
you are connected to only one service provider (i.e. one Remote Connector) then an asterisk in both entries would be sufficient and would cause the Connector to send every message to that one destination. Otherwise create the detailed entries as necessary. The Sender ID is only used by service providers to specify the necessary information for forwarding (re-routing) of messages.

The example in Figure 16 causes the connector to forward all messages with a BuyerID 222222 and a SellerID 888888 to the connector with the Station ID urn:autogration:de:xyz:berlin:001. In the example of Figure 17, the Connector will send any outbound message to the outbound connection defined by urn:autogration:pt:inescporto:porto:002.
Workflows and User Setup

If the business process requires manual intervention to take place before a message is sent out or after a message has been received (for instance, if it is necessary to attach documents to an outgoing message or to have access to documents from an incoming message) the Connector provides the ability to define workflows. Since different users might be responsible for different actions, a basic user management has been implemented as well.

User management

The Connector comes with two pre-defined accounts: an admin account and a user account. The admin account (password is admin) has access to all functions of the Connector and can change the settings whereas the user account (password is user) has a more limited functionality.

If necessary, the user account can be changed, or other users can be created, in order to assign specific tasks to different users. These accounts are also used to distribute notifications, for instance, regarding tasks that have been accomplished by the Connector or by errors that have occurred internally in the Connector.

Select WORKFLOW/Users to access the user management interface.

If necessary use the Add or Edit button to add or change an existing user account.

Especially, if you want to enable user notification by email you must enter the email address and the server used to send the emails (see Figure 19).

---

2 Password of these pre-defined accounts (admin and user) should be changed as soon as possible.
Setup User actions
Workflow configuration is used to define actions to be carried out on messages. Currently, these are the following types of applicable actions:

- Attach documents to an outgoing message
- Extract attachments from a received message

Select Add User Action to define a new action (see Figure 21).
Figure 21

Process: Select outbound or inbound (user action will be done in outbound or inbound messages)

Message: select the message type the action is applicable to

Action: describe the action

User: select the user who is responsible to carry out the action

Finally, save the specification.

The Action table will be updated accordingly (see Figure 22).

Figure 22

Setup User notifications
Workflow configuration is also used to define notifications that are triggered by the Connector when the following events arise:

- An action was successfully accomplished by the Connector on a given message;
- An error was raised by the Connector during the processing of a given message.

Select Add Notification to define a new notification.
Then provide the following data items:

**Process:** select outbound or inbound process (the notification will be triggered in the outbound or inbound process);

**Message:** select the message type that the notification is applicable to;

**Notification Type:** select the type of notification you want to define;

**Language:** select the language that will be used on the notification (currently, the Connector supports the following languages: English, German, French, Spanish, Italian, Dutch and Portuguese);

**Users To Notify:** select the user(s) that will receive the notification.

Finally, save the specification.

The Configuration table will be updated (following Figure 22 represents a situation where two notifications were specified, one for the inbound process and another for the outbound process).
Create a connection for manual download/upload of messages
The following instructions are based on the assumption that your local computer acts only as a client and you want your local Connector to receive messages from a locally accessible file folder (IMPORT folder) and, inversely, you want your local Connector to send messages to a locally accessible file folder (EXPORT folder).

In this mode, any auto-gration Message dispatched by your Connector and stored in the EXPORT folder will have to be uploaded to the final remote computer destination. Inversely, any auto-gration Message that you download from a remote computer source should be placed in the IMPORT folder. Your Connector will then process that auto-gration Message.

Setup the outbound connection(s)
Select CONNECTIONS/Outbound Connections.

You may edit an existing outbound connection or you may create a new outbound connection. Whatever the option, you will have to identify the file folders you want your Connector to use when dispatching outgoing Messages (EXPORT folder) and incoming Messages (IMPORT folder). These folders must be locally accessible before creating/editing the outbound connection. The next Figure shows an example, where only the following fields are applicable:

Station ID: is the station ID of your remote partner / service provider.

TransportProtocol: identifies you are creating a folder-based outbound connection.

RemoteServiceName: identifies a locally accessible EXPORT folder.

FolderForDownloadedMessages: identifies a locally accessible IMPORT folder.

Set Test Indicator: if ticked, all interchanges are marked as test. Use this for the initial test / setup period and unselect the indicator once you change to operational mode.

Enable Dispatch ...: this will cause messages to be stored immediately on the EXPORT folder once placed in the outbound folder.

Enable Periodic ...: will cause the Connector to process inbound Messages available in the IMPORT folder.
Test the outbound connection
Select CONNECTIONS / Check Connections and click Check Connections button.

If the setup is correct, you will see an OK under REMOTE HOST CONNECTION and REMOTE SERVICE.

OK under REMOTE SERVICE indicates that your Connector can access the EXPORT folder. If there is an error in the REMOTE SERVICE column, the most plausible reasons are the following:

- You entered a wrong path for the file folder.
- Connector does not have the required access permissions (read and write) to use one of the file folders.

Set the message routing table
Please apply the previous „Set the message routing table“ section.
Using the Connector as a Server

The Connector may work in the following modes:

- Client-only mode;
- Client and server mode;
- Server-only mode;
- Forwarding mode.

Client-only mode is the default when you install the Connector (see section Configure the Connector). In this mode, data exchange with other Connectors on the Internet (remote connectors) will always be initiated by your Connector (your Connector can't be called by others on the Internet) and you will need to define one outbound connection for each remote connector. No inbound connections should be defined.

In the client and server mode, the Connector accepts data exchanges initiated by other Connectors on the Internet (your Connector can be called by remote connectors running on the Internet, i.e. other business partners can actively push messages to your station). In this mode, you should define one inbound connection for each remote connector that will push messages to your station in addition to the outbound connections (defined for the client mode).

In server-only mode, the Connector has only inbound connections, i.e. all your business partners act as clients.

In the client and server mode, your Connector accepts incoming connections through the HTTP and HTTPS protocols. The recommended protocol is HTTPS as data exchange through HTTP is not secure.

Forwarding mode is a “client and server mode” where the Connector forwards each inbound message to an outbound connection. That is, each inbound message received through one of its inbound connections is forwarded/routed to the outbound connection defined by the routing table defined inside the Connector. This mode is intended to aid the development of software in B2B Interoperability Platform environments.

Setup an HTTP inbound connection

If you need to configure your Connector in the client and server mode (including the forward mode), the first step in the configuration process is to configure the Connector to be accessible through the HTTP protocol.

After installing the Connector as described in previous sections (namely the Configure the Connector section), you will need to create an inbound connection for each possible remote Connector. You should select the CONNECTIONS/Inbound Connections in the user interface and press the Add button.
In the Inbound Connection form, provide the following data elements:

- **StationId** - StationID of the remote Connector that will push messages to your Connector;
- **RemoteHostName**:
  - host name or IP address of the remote Connector if it has a fixed IP address or host name;
  - the symbol ",", (asterisk) to allow incoming connections from any host on the Internet (regardless of its IP address or host name).
- **Password** – password that will be used to authenticate incoming connections (you will need to supply this password to the Administrator of the specific remote Connector so that he defines an outbound connection with that password).

After this configuration, your Connector can be called by the identified remote Connector.

Setup an HTTPS inbound connection

To use the recommended HTTPS communication protocol, you have to install a security certificate to enable the server authentication and SSL/TLS encryption. The certificate must contain a private key. More details about certificates are available e.g. at [http://forum.odette.org/repository/odette-ca-help.pdf](http://forum.odette.org/repository/odette-ca-help.pdf).

The Connector is distributed with a dummy certificate. In the CONNECTIONS/Server PrivateKey screen select the dummy certificate and delete it. You can also delete the odetterootcert and the odetteissuingcert if your server certificate has not been issued by the Odette CA.
Then add your own certificate including the private key. Such a certificate is stored in a keystore file (*.ks, *.jks, *.jceks, *.p12, *.bks and *.ubr are supported formats).

First, provide the password for the keystore and for the private key.

Click Save and use the next dialogue to select and upload the keystore file.
After the successful import, the Connector’s keystore contains the Security certificate with the private key and – optionally – the certificates of the issuing CA and root CA. Your Connector is then ready to act as a server for HTTPS connections. However, you should now restart the Connector, i.e., stop and start it.

The last step in the HTTPS setup is to create an inbound connection for each remote Connector (please follow the same steps as identified in the “Setup an HTTP inbound connection” subsection).

**Important note:**

You will need to send your **Public Key Certificate** (i.e. the one you have downloaded from the issuing CA) to your business partner, who acts as a client. He has to import this certificate and the certificates of the issuing CA and root CA into his client keystore (CONNECTION/Certificates).

Make sure that you send only the public key certificate!

**Activate the forwarding mode**

To activate this working mode in the Connector, you must:

1. Edit the csc-settings.properties file and add to it the following line:
   
   `autogration.remoteconnector.active=true`

2. In the same file, make sure you have the following specification (delete any similar specification you may find in the file):
   
   `autogration.messagedispatcher.sleeptime=30`

3. Specify all the needed inbound and outbound connections.

4. Specify the appropriate routing entries in the routing table, so that the Connector knows where to forward any inbound message.

5. Restart the Connector (i.e. stop and start it).
Internal configuration of the Connector
This chapter aims to identify the low level controlling aspects of the Connector. It describes how the Connector may be further customized to a given ICT environment. The information given here is very technical and targets software engineers and ICT administrators.

Major software artefacts
The connector is composed by the following major software elements:

<table>
<thead>
<tr>
<th>Software artefact</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>„data/db” folder</td>
<td>This folder contains the default relational data base (HSQLDB) used by the Connector</td>
</tr>
<tr>
<td>„data/archive” folder</td>
<td>By default, this folder is used to store all archived messages</td>
</tr>
<tr>
<td>„data” folder</td>
<td>Remaining subfolders are used by the Connector</td>
</tr>
<tr>
<td>„tomcat-7.0.27” folder</td>
<td>This folder contains the default application server (Apache Tomcat) that runs the Connector web application</td>
</tr>
<tr>
<td>csc-keystore.jks and csc-truststore.jks files</td>
<td>These two files are the default files that constitute the key store and trust store of the Connector (they are also used by the Apache Tomcat)</td>
</tr>
<tr>
<td>csc-hibernate.properties file</td>
<td>This configuration file specifies which relational data base is used by the Connector (by default it is a HSQLDB data base)</td>
</tr>
<tr>
<td>csc-settings.properties</td>
<td>This configuration file specifies data items that control the way the Connector works</td>
</tr>
<tr>
<td>csc-connections-routings.xml</td>
<td>This configuration file is the place where all inbound and outbound connections, as specified by the Administrator in the user interface, are saved.</td>
</tr>
<tr>
<td>csc-workflow.xml</td>
<td>This configuration file is the place where all user actions and notifications, as specified by the Administrator in the user interface, are saved.</td>
</tr>
</tbody>
</table>

The csc-hibernate.properties file
This file defines all the controlling items of the Hibernate framework, the software element in the Connector that is responsible for managing data in a relational data base. By default, this configuration file defines the HSQLDB data base but another relational data base may be configured instead (for instance, PostGreSQL, MySQL, ...).
The following table identifies the purpose of some controlling items:

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>hibernate.connection.url</td>
<td>Defines the URL of the database the Connector will use</td>
</tr>
<tr>
<td>hibernate.connection.username</td>
<td>Defines the user name that will be used to access the database</td>
</tr>
<tr>
<td>hibernate.connection.password</td>
<td>Defines the corresponding password</td>
</tr>
<tr>
<td>hibernate.connection.driver_class</td>
<td>Defines the driver that will be used to access the database</td>
</tr>
<tr>
<td>hibernate.dialect</td>
<td>Defines the dialect to be used</td>
</tr>
</tbody>
</table>

Figure 32
The csc-settings.properties file

This configuration file specifies all the controlling items of the Connector’s core.

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>autogration.mystationid</td>
<td>Defines the StationID of the Connector</td>
</tr>
<tr>
<td>autogration.messagedispatcher.sleeptime</td>
<td>Defines the polling frequency for internal message management functions</td>
</tr>
<tr>
<td>autogration.messagedispatcher.getmessagesfromoutboundconnections</td>
<td>Defines the polling frequency for the message fetching mechanism regarding remote connectors</td>
</tr>
<tr>
<td>autogration.erpadapter.callerid</td>
<td>Defines the identifier that the local ERP must supply to the Connector in order to call its web service interface</td>
</tr>
<tr>
<td>autogration.erpadapter.password</td>
<td>Defines the corresponding password</td>
</tr>
<tr>
<td>autogration.simplemessage.messagetype.jitdeliveryinstruction.sellerid.xpath</td>
<td>Defines the XML element used by the Connector to retrieve the SellerID from an auto-gration Message of type</td>
</tr>
</tbody>
</table>
**Internationalization support**

The user interface of the Connector has internationalisation support for multiple languages. Currently, the following languages are available: English, German, French, Spanish, Italian, Dutch and Portuguese. By default, the Connector’s user interface uses the preferred language as defined by your Internet browser. If the Internet browser defines a language that does not exist in the Connector, English language is used.

Other languages may be easily added to the Connector. All you have to do is:

1. Peek the `"tomcat-7.0.27\webapps\autogration\WEB-INF\classes\eu\autogration\car\simpleconnector\ui\messages.properties"` file and copy its contents to a new file, in the same location, with the name `"messages_xx.properties"`, where `"xx"` corresponds to the international code of the new language (2-letter language codes defined by ISO 639-1 Code), for which you want to produce a new translation.

2. Translate all the terms defined by the `"messages_xx.properties"` file.

3. Stop and start the Connector application.

4. Check the user interface and go back to step 2 if more changes are required.

Notice: keep a backup of the file(s) you have created/changed by the above procedure.

**Notification templates**

All the notifications generated by the Connector are created from an appropriate template. The available templates reside at the `"tomcat-7.0.27\webapps\autogration\Mail_TMPL"` folder and are specific for a given language. If you do need to create notification templates for a new language (or change the ones already existing), all you have to do is:

1. Peek the file, e.g. `"action_done_default.ftl"` and copy its contents to a new file, in the same location, with the name `"action_done_xx.ftl"`, where `"xx"` corresponds to the international code of the new country for which you want to produce a new notification (2-letter language codes defined by ISO 639-1 Code).

2. Translate all the terms defined by the `"action_done_xx.ftl"` file.

3. Stop and start the Connector application.

---

3 Can be used analogous for other messages without a SellerID

4 Can be used analogous for other messages without a BuyerID
Notice: keep a backup of the file(s) you have changed by the above procedure.

**Customize the Archiving function**

The Connector supports the archival of all sent and received messages (independently of this feature all messages sent/received by the Connector are kept in a local database). This is accomplished in the TRANSACTIONS area of the user interface, by selecting with the right hand button a set of inbound or outbound messages and by choosing the option “Archive Message ...”. By doing this, the selected messages and all their possible annexes are saved as separate files in a given locally accessible folder. By default, this folder is the “data/archive” folder.

Customization of this mechanism allows you to change the folder used to maintain the archive and to set the format to apply on the file names. For this, you need to edit the XML “<ArchiveDef>” element, present in the csc-workflow.xml file (stop and start the service after changing this file). The default contents of this file, after installing the Connector in a “…/auto-gration-connector-win32” folder, is the following:

```xml
<ArchiveDef>
  <archiveFolder>D:/auto-gration-connector-win32/setup/../data/archive</archiveFolder>
  <archiveFileNameTemplate>${transaction_type}-${message_type}-${interchange_id}-${document_id}</archiveFileNameTemplate>
</ArchiveDef>
```

The element “archiveFileNameTemplate” can refer to the following variables:

- ${message_type}
- ${sender_id}
- ${receiver_id}
- ${buyer_id}
- ${seller_id}
- ${interchange_id}
- ${document_id}
- ${document_issue_date}
- ${transaction_time_stamp}
- ${transaction_type}

The usage of the variables in the archiveFileNameTemplate element allows the customization of the way files are named in the archive folder.
Updating the connector with a new version (Windows)

Since version 2.7.4, the Connector allows you to check whether the auto-gration consortium has made available new releases of the software. This is available in the ABOUT area of the user interface.

The Connector is maintained by the auto-gration Joint Working Group in order to manage new functional requirements, fix errors and enhance the usability of the software. Utmost attention will be paid to the downwards compatibility of succeeding versions so that setup specifications and data will be available and accessible after an update.

In order to update an existing installation, you must proceed as follows (we assume that your existing Connector is installed in folder \auto-gration-connector-win32).

Preparation
1. Backup the existing installation (copy \auto-gration-connector-win32 to an appropriate place in your computer).

Conducting the update
2. Stop the service by running the stop-service.bat in the tomcat-xxx folder.
3. Un-install the service by running uninstall-service.bat as an administrator.
4. Download the new version of the connector (in the form of a zip file).
5. Extract the ZIP file into the same folder as the previous one.
   If your installation is in \auto-gration-connector-win32 then extract the ZIP archive file into \auto-gration-connector-win32.
6. Run the setup.bat in the application directory, \auto-gration-connector-win32, and enter the required data for StationID, proxy settings, etc (for details see section Run the setup).
7. Install the service (run script install-service.bat in the tomcat... folder).
8. Start the service (run script start-service.bat as administrator).

Post-processing
9. Log onto the Connector as administrator.
10. Check the connections and workflows.
Updating the connector with a new version (linux)
Since version 2.7.4, the Connector allows you to check whether the auto-gration consortium has made available new releases of the software. This is available in the ABOUT area of the user interface.

The Connector is maintained by the auto-gration Joint Working Group in order to manage new functional requirements, fix errors and enhance the usability of the software. Utmost attention will be paid to the downwards compatibility of succeeding versions so that setup specifications and data will be available and accessible after an update.

In order to update an existing installation, you must proceed as follows (we assume that your existing Connector is installed in folder `/user/autogration/auto-gration-connector-linux32`).

Preparation
1. Backup the existing installation (copy `/user/autogration/auto-gration-connector-linux32` to an appropriate place in your computer).

Conducting the update
2. Stop the service by running the `stop-daemon.sh` in the tomcat-xxx folder.
3. Un-install the service by running `uninstall-daemon.sh`.
4. Download the new version of the connector (in the form of a tar file).
5. Extract the ZIP file into the same folder as the previous one.
   If your installation is in `/user/autogration/auto-gration-connector-linux32` then extract the tar archive file into `/user/autogration/`
6. Make sure the shell scripts are marked as executable. If they are not, you can for instance run `chmod -R +x /user/autogration/auto-gration-connector-linux32/*.sh` in a console.
7. Run the `setup.sh` in the application directory, `/user/autogration/auto-gration-connector-linux32` and specify the required data for StationID, proxy settings, etc (for details see Run the setup).
8. Install the service (run the script `install-daemon.sh` in the tomcat... folder)
9. Start the service (run the script `start-daemon.sh`).

Post-processing
10. Log onto the Connector as administrator.
11. Check the connections and workflows.