X/P Messenger 5.0

Version: 1

Current date: 2025-10-29

Table of Contents

1. Installation Guide

1.1. Installation procedure

1.1.1. Windows

The PONTON XP Messenger is delivered as a zip file which needs to be unpacked to a directory of your choice, the configuration files have to be edited manually.

Prerequisites

Please define and verify certain parameters such as the following before proceeding:

- You need a database installed (either locally or remote)

Step 1: Copy and unpack the .zip messenger installation file in your chosen directory.

To avoid errors during the installation procedure please define and verify certain parameters such as the following before executing the installer as a windows service:
Service installer configuration in launcher\conf\wrapper.conf

```
set.NTSERVICE_NAME=pontonxpmessenger
# This value has to be a unique service identifier on the Windows system. So if there are multiple Messenger instances on this system, you need to modify this.
```

Database configuration (as per property definition in the section 'Database Connection') in launcher\conf\wrapper.conf

```
# The JDBC-URL of database

set.default.DATABASE_URL=

# the user to be used for database connection

set.default.DATABASE_USER=

# the encrypted password of database user.

set.default.DATABASE_PASSWORD=
```

⚠️ It is required to set the database URL, USER and PASSWORD before the initial startup.

[Info Icon] Only once during the messenger startup your pre existing configuration from the existing folder xpmessenger-.../config/ will be scanned and automatically stored into this database as long as there is no existing configuration in this database. Thereby, make sure

that the database URL is exlusive for your pontonxp messenger.

Step 2: The Messenger can then also be installed as a windows service. To do so please execute installService.bat in the freshly unpacked PONTON X/P Messenger installation.

A command line window will show up on the screen, stating that the PONTON X/P Messenger has been installed successfully.

wrapper | PONTON X/P Messenger installed.

Step 3: Before starting the PONTON X/P Messenger as an installed service:

Messenger database preparations

1) The database must be created and the database user assigned to PONTON X/P Messenger needs DB-Admin rights, which allows to create/change tables, sequences, indices and foreign keys.

2) The required database tables will be created by PONTON X/P Messenger automatically on startup. Further details can be found in section "Database Update" inside of PONTON X/P Migration Guide.

3) Furthermore a compatible database driver will be required by the PONTON X/P Messenger. Please save a copy of the required driver in the folder lib_ext of the messenger installation.

Step 4: Start PONTON X/P Messenger as an installed service. If any errors occur during startup, this will be logged in the data\log\wrapper.log

1.1.2. Linux

The PONTON X/P Messenger is delivered as a zip file which needs to be unpacked to a directory of your choice, the configuration files have to be edited manually.

Prerequisites

Please define and verify certain parameters such as the following before proceeding:

- You need a database installed (either locally or remote)

Log in to the Linux machine with the user intended to run the messenger. Ensure that this user has the right to read, write und execute!

Step 1 : Copy and unpack the .zip messenger installation file in your chosen directory.

Step 2 : Before proceeding with the installation process please ensure that the **PONTON XP /pontonxp** as well as the **PONTON XP /launcher/linux-.../wrapper** files are executable.

Step 3 : Configure the necessary parameters in pontonxp :
Installation configuration in pontonxp

```
...
APP_HOME="." # Ensure that this location refers to your PONTON XP messenger installation.
...
```

Step 4 : Database configuration (as per defined parameters in the section 'Database Connection') in **launcher\conf\wrapper.conf**

```
# The JDBC-URL of database

set.default.DATABASE_URL=

# the user to be used for database connection

set.default.DATABASE_USER=

# the encrypted password of database user.

set.default.DATABASE_PASSWORD=
```

⚠️ It is required to set the database URL, USER and PASSWORD before the initial startup.

[Info Icon] Only once during the messenger startup your pre existing configuration from the existing folder xpmessenger-.../config/ will be scanned and automatically stored into this database as long as there is no existing configuration in this database. Thereby, make sure that the database URL is exlusive for your pontonxp messenger.

Step 5 : Before starting the PONTON X/P Messenger please set up your database

Messenger database preparations

1) The database must be created and the database user assigned to PONTON X/P Messenger needs DB-Admin rights, which allows to create/change tables, sequences, indices and foreign keys.

2) The required database tables will be created by PONTON X/P Messenger automatically on startup. Further details can be found in section "Database Update" inside of PONTON X/P Migration Guide.

3) Furthermore a compatible database driver will be required by the PONTON X/P Messenger. Please save a copy of the required driver in the folder lib_ext of the messenger installation.

Step 6 : Start the messenger service

- Manual start

/pontonxp start

Step 7 : (optional): Install as systemd service

- Consider moving the pontonxp folder to a non-user and non-system directory like /usr/share/
- To run PONTON X/P Messenger as a service, we recommend to create a dedicated user without login shell for this use.
- Make this user owner of the pontonxp directory including all subdirectories

To install PONTON X/P Messenger as systemd service run the script launcher/systemdService as super user (root). It offers the following parameters:

- **install username** - Installs the systemd service under the specified username. Installs the configuration file pontonxp.service into /etc/systemd/system and enables the service.
  Example:

```
1 | sudo ./systemdService install pontonxp
```

- **remove** - Removes the systemd service if it is installed. Stops the service, disables it, and deletes the configuration file from /etc/systemd/system.
- **status** - Shows the current status of the service, including whether it is installed and active. Displays systemd information like activation status and logs.
- **start** - Starts the service if it is installed. If the service is already running, it remains unchanged.
- **stop** - Stops the service if it is installed and actively running. Prevents further execution until manually started again or upon system startup.

Both methods: If any errors occur during startup, this will be logged in the data/log/wrapper.log

1.2. Database Setup

1.2.1. General

Since version 5.0 of Messenger, all "text" columns in database should support UnicodeCharacters. So the database must be created using corresponding CharacterSets and Collations. Please refer to documentation of corresponding database. During an update to Messenger version 5.0 the data type of all "text" columns is changed to unicode support. Additionally the Messenger checks JDBC-URL-Parameters and database settings to ensure unicode is supported properly.

1.2.2. Database Driver (JDBC)

Due to the upgrade to JAVA >= 21 the latest JDBC database drivers must be used.
Copy the database driver to the folder **lib_ext**\.

1.2.3. Database Connection

The Database Connection parameters can be configured via local file (**/launcher/conf/wrapper.conf**) or as externally set **Environment Variables**. [Info Icon] If environment variable as well as property values are set, then the values from the environment variable will be used by the application. The following variables / properties are available:

wrapper.conf property	Environment Variable	Description	Default Value
set.default.DATABASE_URL=	DATABASE_URL	The JDBC-URL to connect to database	
set.default.DATABASE_USER=	DATABASE_USER	The user for DB connection	
set.default.DATABASE_PASSWORD=	DATABASE_PASSWORD	The encrypted password of the user for DB connection	
set.default.DATABASE_CONNECTIONS_MIN=	DATABASE_CONNECTIONS_MIN	The minimum number of DB connections established	2
set.default.DATABASE_CONNECTIONS_MAX=	DATABASE_CONNECTIONS_MAX	The maximum number of DB connections established	10
set.default.DATABASE_CONNECTION_TIMEOUT=	DATABASE_CONNECTION_TIMEOUT	The maximum timeout for DB connection (in seconds)	300 (s)
set.default.DATABASE_LOGGING_SQL=	DATABASE_LOGGING_SQL	The maximum timeout for DB connection (true/false)	false

1.2.3.1. Encrypting database password

The database password should always be set encrypted. To encrypt the password a shell-script is installed (**sql/encryptPW** or **sql/encryptPW.bat**) which takes the clear text password and returns the encrypted value

sql/encryptPW

```
1 | > cd sql
2 | > encryptPW myDatabasePassword
3 | encrypted pw: AP8AdxmHIsmqPKn7rHO5i3mch8f3GMNL/olTwDVWNvo5rg4=
```

1.2.4. Database URL

For each of the supported database types the URLs can be defined with JDBC parameters as follows:

1.2.4.1. MS-SQL

https://go.microsoft.com/fwlink/?linkid=224757

launcher/conf/wrapper.conf

```
1 | set.default.DATABASE_URL=jdbc:sqlserver://SERVER:1433;database=DBNAME;
encrypt=true;trustServerCertificate=true;
```

JDBC-Parameter	Description	Recommendation
encrypt	The connection to database is encrypted.	Set to encrypt=true
trustServerCertificate	Allows self-signed server certificates	Set to trustServerCertificate=true
sendStringParametersAsUnicode	Send QueryParameterValues as unicode, to use corresponding index properly, which improves request performance.	⚠️ Until version 4.6 this parameter should be set to false, because columns and indices contain non-unicode content. sendStringParametersAsUnicode=false Since version 5.0 this parameter should be omitted or set to true, because content is now unicode encoded. sendStringParametersAsUnicode=true
characterEncoding	The character encoding to use.	Omit or set to characterEncoding=UTF-8
useUnicode	Use unicode characters.	Omit or set to useUnicode=true

1.2.4.2. Oracle

https://download.oracle.com/otn-pub/otn_software/jdbc/233/ojdbc11.jar

launcher/conf/wrapper.conf

```
1 | set.default.DATABASE_URL=jdbc:oracle:thin:@SERVER:1521:DBNAME
```

JDBC-Parameter	Description	Recommendation
characterEncoding	The character encoding to use.	Omit or set to characterEncoding=UTF-8
NLS_LANG	The language used.	Omit or set to value ending with AL32UTF8. F.e. NLS_LANG=AMERICAN_AMERICA.AL32UTF8

1.2.4.3. MySQL

https://dev.mysql.com/downloads/connector/j/8.3.html

launcher/conf/wrapper.conf

```
1 | set.default.DATABASE_URL=jdbc:mysql://SERVER:3306/DBNAME?autoReconnect=true&useSSL
=true&allowPublicKeyRetrieval=true
```

JDBC-Parameter	Description	Recommendation
characterEncoding	The character encoding to use.	Omit or set to characterEncoding=UTF-8

JDBC-Parameter	Description	Recommendation
useUnicode	Use unicode characters.	Omit or set to useUnicode=true

1.2.4.4. PostgreSQL

https://jdbc.postgresql.org/download/

launcher/conf/wrapper.conf

```
1 | set.default.DATABASE_URL=jdbc:postgresql://xpdb:5432/integration
```

JDBC-Parameter	Description	Recommendation
characterEncoding	The character encoding to use.	Omit or set to characterEncoding=UTF-8
client_encoding	The encoding to use	Omit or set to client_encoding=UTF8

1.2.5. Database setup/update

⚠️ Since PONTON X/P Messenger 4.6.0 the structure of database is checked on startup and automatically updated, if necessary. For this the assigned database user needs admin rights on database, to create/update/drop tables, sequences, indices and foreign keys. During "normal" operation mode, the admin rights are not required anymore. There are three possibilities to update the database:

1. The required admin rights are assigned to the database user permanently (see section “Required database rights” in the chapter Troubleshooting)
2. The admin rights are assigned to the database user only temporary and revoked after update process (see section “Required database rights” and “Manual database setup/update” in the chapter Troubleshooting)
3. The database user has only the rights for operational mode. After installing the new version, an update script is generated, which is executed by a database administrator with extended rights (see section “Manual database setup/update” in the chapter Troubleshooting)

1.3. Importing the X/P configuration from an existing messenger

1.3.1. From a messenger version between 3.1 and 4.6.

Please refer to the 'Migration Guide' for details

1.3.2. From a messenger version 5.0 and higher

Go to: **MONITOR** > **Dashboard**

Click on the download config files icon ⬇ to download the config files to a download folder in your local system. This results in a file which contains the complete messenger configuration. This exported configuration file can then be imported into a new messenger or into a new database via the UI function ↑.

> [Info Icon] This file is specific for each messenger version. Hence, importing the configuration in a new messenger is only possible if the export and import are for the same messenger version.

1.4. Installing multiple Messenger instances on the same system

1.4.1. Installation

Each Messenger instance has to be installed in a dedicated folder. It is required to have the Messenger instances connected to an external database.

The following port values need to be changed in the WEB GUI:

Port Name	**default value**
Web GUI + REST API	8443
Adapter-API v1	8080
Adapter-API v2	2600

1.5. Error-MaintenanceMode for handling port conflicts

When a port conflict is detected during startup, the Messenger will start in “Error-MaintenanceMode”, so that it is possible to adjust the ports in the GUI. The “Error-MaintenanceMode” is visualized with a fixed color adjustment and changed label of Messenger Name:

If the GUI port had a conflict the Messenger will search for a random free port and start the GUI with this port. The random port can be found in the console or wrapper.log.

```
jvm 2    |
jvm 2    |     (C) 2000-2025 PONTON GmbH
jvm 2    |
jvm 2    |     The AdminTool is available on:
jvm 2    |       https://localhost:18445
jvm 2    |
jvm 2    |     The REST API is available on:
jvm 2    |       https://localhost:18445/api/swagger-ui
jvm 2    |
jvm 2    | ************************************************************************
```

2. Initial Setup

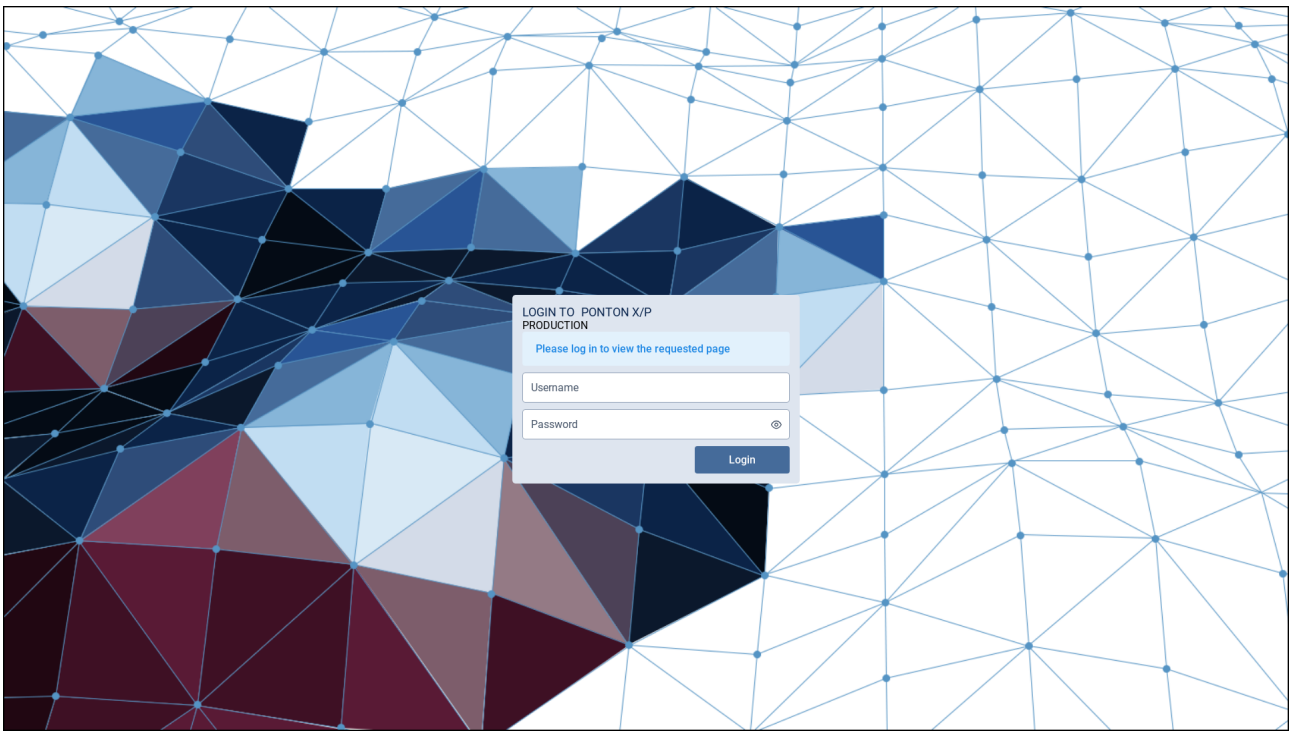
2.1. How to get started

2.1.1. Logging in

Open your web browser and enter the following URL:
https://<hostname>:8443/

or

https://localhost:8443/ if the Messenger is running on the local machine!
This will bring up the login screen, allowing you to log in to the Ponton X/P Administration Tool:



⚠ The initial user name and password depends on the type of installation.

For an on premise installation the default values are:

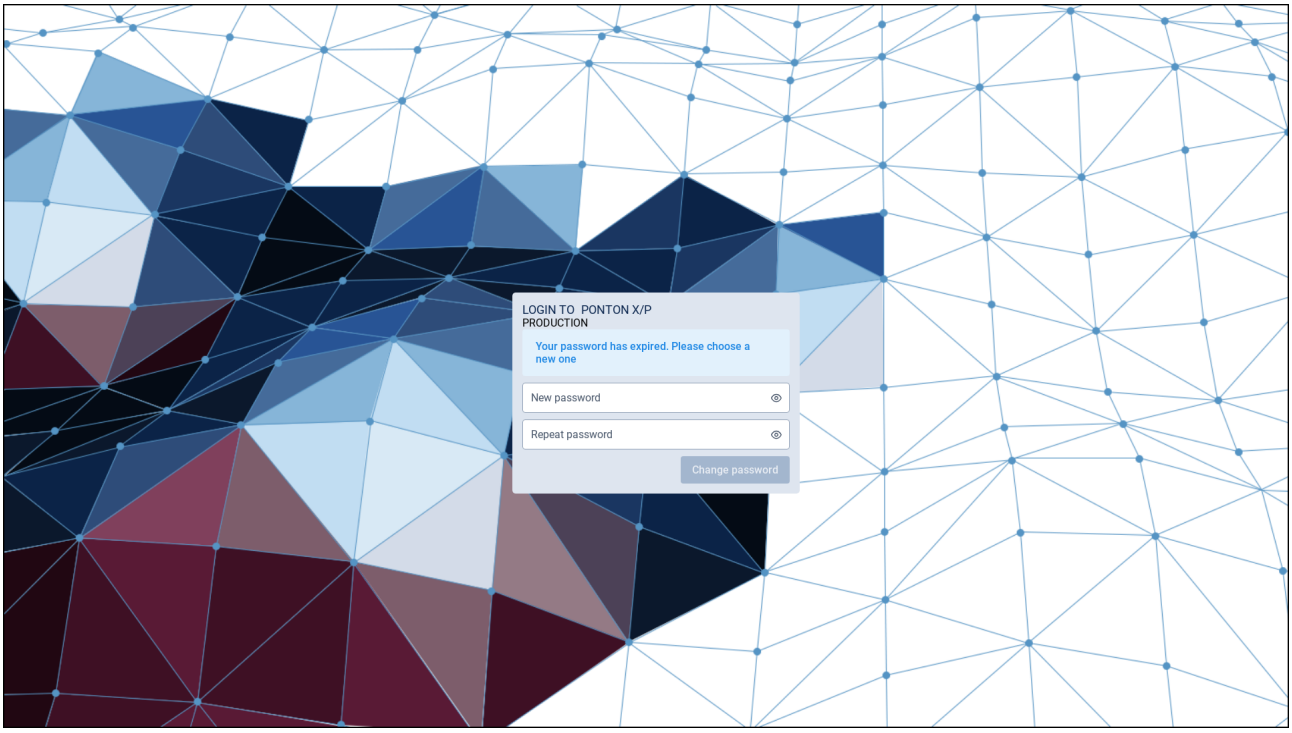
User: xpadmin
Password: xppass

For an AWS installation the default values are:

User: xpadmin
Password: (EC2 instance_id)

The initial user login values must be changed on first login to prevent unauthorized access to the Administration Tool. After entering the username and password and clicking on the "*Login*" button you will be asked to enter a new password and repeat it. Once you entered valid and matching

passwords click on the "*Save Password*" button.



2.1.2. Using the Navigation Bar

Click on the icons on the navigation bar to navigate the main pages.

2.1.2.1. Main Navigation (left)

Area	Symbol	Description	Subnavigation	Description
Monitor			• Dashboard	
			• Adapter Status	
			• Cluster Status	
			• TLS-Certificate Status	Overview of all TLS server certificates and their status
			• Partner-Certificate Status	Overview of all remote partner certificates and their status
Messages		View message details and delete Messages		

Area	Symbol	Description	Subnavigation	Description
Messenger			• Partner	Create and edit local / remote Partner; Add and manage Partner Certificates
			• Agreements	Add, configure, delete Agreements
			• Settings	Configure general Messenger settings; Add and manage Server Certificates
			• Activation	Get licence info; Send activation requests; Install activation and licence
			• Schema	Install or update SchemaSets
			• Multicast Rules	Configure rules for sending message duplicates
Listener		Add, configure, delete Listener; Add and manage Listener certificates and Client Certificates		
Hotfolder		Add, configure, delete Hotfolder		
Http Adapter		Add, configure, delete Http Adapter		
Test Adapter		Send test messages; Ping partners		
User Admin		Change security settings and settings of others user		

2.1.2.2. Main Navigation (right)

2.1.2.3. Set Messenger instance name

On the navigation bar you see the **Messenger Instance Name**, which can be configured to display a name that easily identifies the system. Further you see how many days are left until the licence expires as well as the user name of the user who is logged-in.

Area	Symbol	Description	Sub-Navigation	Description
User Menu			• User Settings	Change your language settings and your password
			• Logout	Log out of PONTON X/P
Help?		User manuals, link to support portal and 3rd party libraries	• Product Page (external link)	Go to PONTON X/P product website
			• Licence Agreement	View Licence Agreement
			• 3rd Party Libraries	GUI and Java 3rd Party libraries

2.1.3. Need help?

Click on the 

symbol on the right hand side of the navigation bar, which opens a modal window.

Manuals

Click on the document you want to download and the document is downloaded to you local directory on your computer. The following manuals are available:

- Messenger Documentation
- Release Notes
- System Requirements
- Backend Integration Guide
- Adapter Programming Guide

Support

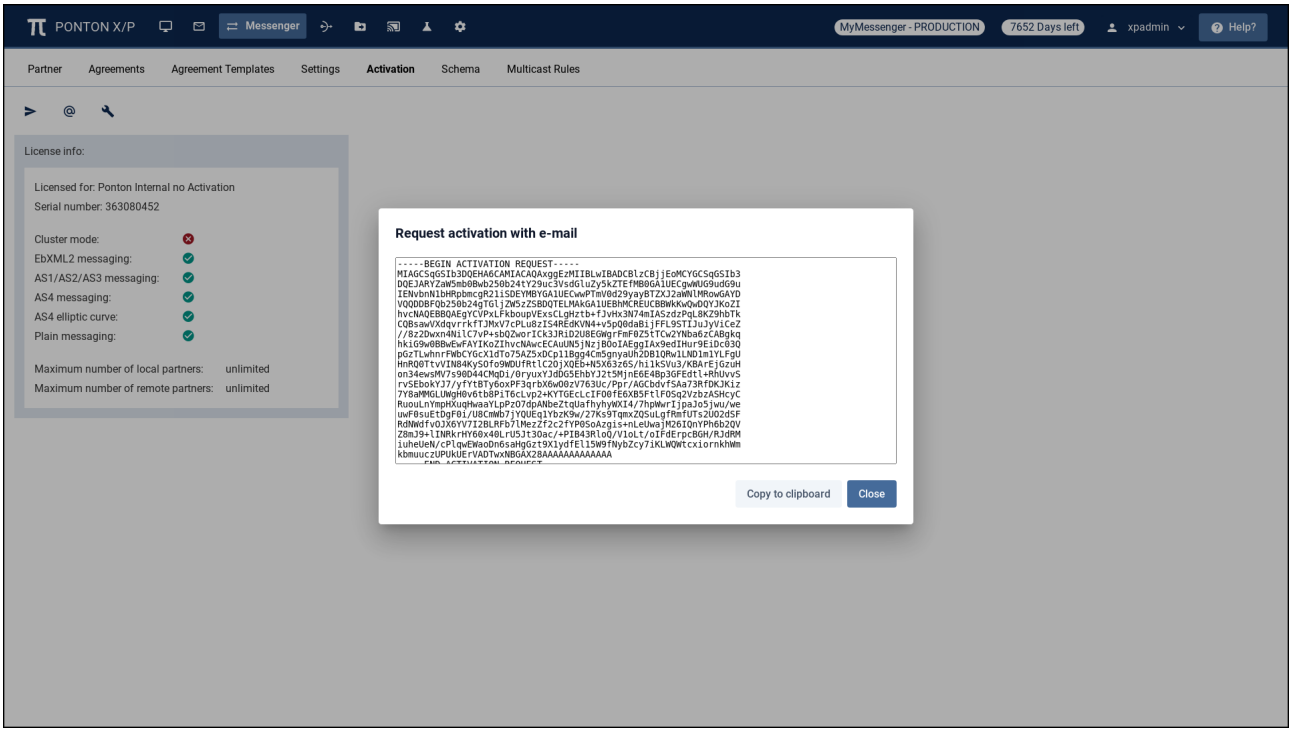
In addition you find a link to the PONTON X/P support portal under "*Support Panel*" and the Product page on PONTON's webside.

Licenses

- List of all 3rd party licences for the UI
- List of all 3rd party Java licences

2.1.4. Activate the software (trial version)

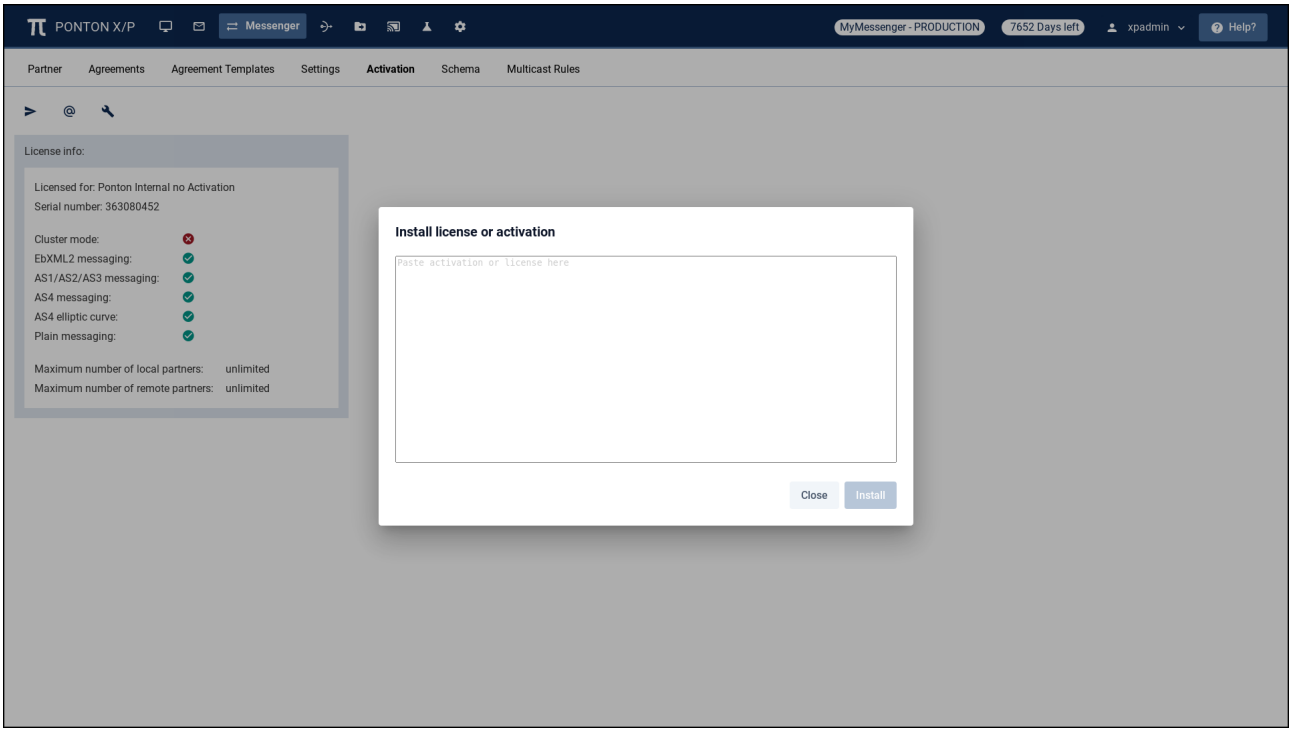
Before proceeding to the communication tests, it is required to activate your Messenger. You can run PONTON X/P Messenger as a trial version for up to 60 days. To activate the trial version, go to **MESSENGER** > **Activation** and click on the "*Mail Activation Request*" @ icon. This will open the Dialog "*Request activation with e-mail*" containing your activation request.



For the trial version, please click on the "*Copy to Clipboard*" button at the bottom of the dialog. This will copy the activation request to your clipboard. Please send the activation request to activation@ponton.de with your e-mail client (e.g. Outlook)

You will receive a reply e-mail containing the activation code for your system. Please copy the complete activation code and click on the "*Install Activation/License*" icon, paste the activation code into the text box of the install dialog and click on the "*Install*" button. The software is now activated.

⚠ When sending your activation request by e-mail, it is important to *copy the complete activation request code*, including the lines "----- Begin Activation Request -----" and "----- End Activation Request -----". The same applies when copying the activation code from the reply e-mail into the Install dialog box. Please also ensure to include the "Begin" and "End" lines.



⚠️ The "Send Activation Request by HTTP" option can only be used after a license has been installed.

2.1.5. Basic configuration

The basic functionality of PONTON X/P is to enable the secure exchange of Messages between business partners. This requires setting up at least two Partner configurations:

- a *Local Partner *(representing your own organization)
- a **Remote Partner** (representing your business partner’s organization)

A Partner profile can be seen as representing the communication capability of the respective Partner. A Partner may, for example, support HTTP(S), SMTP and FTP(S) as transport protocols. An Agreement then restricts the capabilities of two Partners to a choice of options that are supported by both sides. In the case of the transport protocol, the partners might define HTTP as the protocol they want to use. If you use the Adapter notification mechanism, any changes in your Partner configuration will be reported to your Adapters. In practice you will exchange messages with a lot of business partners, so you need to define Remote Partner configurations for each business partner.

[Info Icon] We recommend to initially set up a test installation preferably in a test environment. It might be easier to install two Messengers on separate PCs within your local environment as you avoid firewall restrictions. However, if you want to immediately test with a Remote Partner, please ensure with your technical administration staff that your firewall is configured to allow the necessary connections.

2.1.5.1. Create a local partner

As mentioned above, the Partner configuration distinguishes between **Local** and **Remote Partners** – this distinction indicates whether the Partner refers to a Local Partner within your own PONTON X/P system or to a Remote Partner on an external system. In certain cases, the configuration steps may differ slightly. For example, you can submit a certificate request for a Local Partner, but not for a Remote Partner. In the case of Remote Partners you would receive the certificate from the Partner directly or by downloading the Partner's profile from the Partner Registry.

See chapter Messenger >Partner

⚠ Please ensure that identical Party IDs are used in the sender's as well as receiver's messenger configuration – otherwise there will be errors when you attempt to exchange messages with your partners. Other Party ID types can also be used, for example EIC, Duns Number, GLN (Global Location Number) or URI. For a single partner you can create multiple Party IDs by using different Party ID types which need to be configured separately.

2.1.5.2. Create remote partners

To test your Messenger configuration, a Remote Partner is required.

⚠ When exchanging partner configurations with your business partners please keep in mind that identical party IDs have to be used in the local partner and remote partner configurations. The partner display names and internal IDs, on the other hand, may be different.

	ABC's local partner config.	ABC's remote partner config.	XYZ's local partner config.	XYZ's remote partner config.
Partner display name	**ABC Local**	**XYZ Global**	**XYZ Local**	**ABC Corp**
Internal partner ID	**ABC015** (ERP ID)	**XYZ381** (ERP ID)	**401690** (DB ID)	**494230** (DB ID)
Party ID	**ABC12201**	**XYZ2950A**	**XYZ2950A**	**ABC12201**

See chapter Messenger >Partner

2.1.5.3. Request certificates for remote partners

If you decide to run your initial tests without installing certificates for your partner configurations, please note that the following settings have to be modified to compensate for the absence of certificates.

- Deactivate the **Signing** and **Encryption** options in **Messenger** → **Agreements** → **Configuration** > **Processing**
- Deactivate the **Use XML Signature** option for **EbXml** in **Messenger** → **Agreements** → **Configuration** > **Packager**

Save the changes by clicking on the save icon.

⚠️ A partner certificate will only be accepted after the certificate of the issuing CA (certificate authority) has been installed. Otherwise the trust relationship between the partner and the CA cannot be traced. The certificate for the PONTON CA is automatically included in the default installation. For other certificate authorities you will need to obtain and install the relevant CA certificate. All certificates that you install for one partner will become default certificate in the order of their valid-from date. Alternatively, you can manually select the default certificate and the certificate that should be default when this certificate expires.

See chapter **Certificates**

2.1.5.4. Delete a Partner

See chapter Delete partner(s)

2.1.5.5. Using the Partner Registry

If your communication partners and you have a common Partner Registry then exchanging partner profiles is very simple.

2.1.5.5.1. Import all profiles

To import all available profiles navigate to **Messenger → Partners → Partners Registry** and select one or several Partner with the checkbox on the left hand side in the table row. The number of selected Partners is displayed next to the import icon, then click 'Import all'. This automatically imports all available Partner profiles from the registry into your local Messenger. Although, profiles which may collide within already existing Partner profiles within your Messenger will not be imported to avoid overwriting current Partner profiles.

2.1.5.5.2. Update individual profiles

Partner profiles, which have been modified since the last import are not displaying a green check symbol in the My Partners table. To syncronize the Partner profiles a go to: **MESSENGER * >Partner > My Partner and select one or several partner with the checkbox on the left hand side in the table row. The number of selected partners is displayed next to the syncronize icon. Click on the synchronize icon to start the syncronization process. Alternatively, you could activate the option *"Automatic updates"** to enable your Messenger to update all downloaded Partner profiles periodically as described in the section **Create Remote Partner**.

2.1.5.5.3. Synchronize Partner Profile with the Partner Registry

To synchronize the current Partner configuration with the Partner Registry, go to the Registry tab. If the current partner configuration has not changed since it was last synchronized with the registry, a corresponding message will be displayed.

⚠️ Please note that the Messenger has to establish a connection with the Partner Registry in order to compare the current Partner configuration with the Partner profile stored in the Partner Registry. For this reason you may experience a short delay when you open the

Registry tab.

See chapter **Partner Registry**

2.1.5.6. Set up a partner agreement

When the local as well as remote partner configuration is finished the next step is to define an agreement between these two partners, allowing them to successfully communicate with each other. Select **MESSENGER** on the navigation and than **Agreements** in the sub-navigation bar. Click on the "***Add agreement***" ⊕ icon, which opens the "New Agreement" dialog box. Enter **your local Partner ID** as Partner 1 and **the remote Partner ID** as Partner 2 from the list of available partners. Select an agreement template from the drop-down menu. Then click on the "*Next Step*" button which brings you to the **Agreement Configuration** page. The Names of the two Partners and the selected template is displayed below the sub-navigation bar. Create the agreement with the default settings.

For further information see chapter **Create a new Agreement**

2.1.5.7. Messenger Settings

You can specify how the Messages sent by a Partner will be packaged for transmission and backend processing. It is also possible to define certificates for different packagers such as AS1, AS2, EbXml etc. In that case the agreements created for this partner thereafter will automatically use the packager certificates as defined in the Partner configuration. You can choose between different packaging standards, that offer diverse options to specify whether the relevant packaging elements will be used by this Partner. EbXML and AS1/AS2/AS3 are most widely used. For details on the specific settings please refer to the descriptions of packaging elements in the 'Partner Agreements' section.

⚠ If 'default' certificate is chosen in the packager, the certificate used by the packager will automatically be updated as soon as another certificate is defined as the 'default' partner certificate.

2.1.6. Start communication

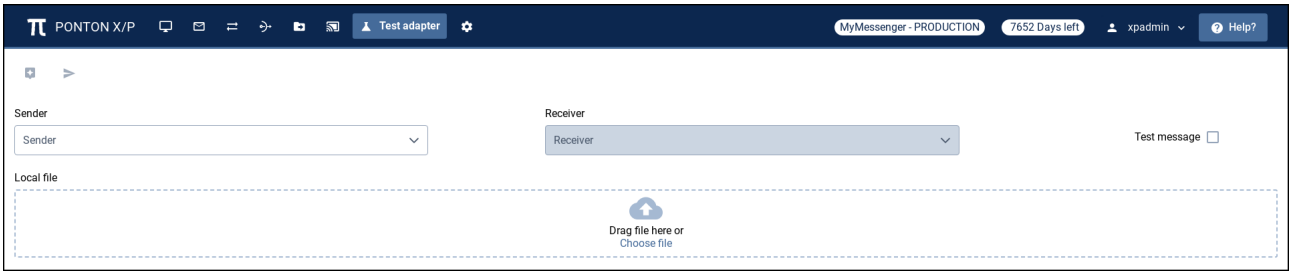
2.1.6.1. Check your proxy settings

In case your Messenger is not meant to communicate with external networks directly and/or there is no proxy available in your network for outgoing messages, you could download and install the PONTON X/P Listener as described in **Listener Configuration** in PONTON X/P Messenger end user documentation.

2.1.6.2. Send a Ping message

PONTON X/P Messenger is delivered with a built in Test Adapter. It can be used to send EbXml Ping messages to test the connectivity between your own messenger and your business partner. Click on **Test Adapter** on the navigation bar to access the test adapter. Please read the section **Test Adapter**

in PONTON X/P Messenger end user documentation for further information.



2.1.7. View Messages in the Message Monitor

Please read the section **Message Monitor**

2.2. Security recommendations

2.2.1. Updating of Java Runtime

In the PONTON X/P distribution the latest compatible Java Version is delivered. It is recommended to update PONTON X/P periodically (every six months). The X/P Messenger patches update the PONTON program code and also the Java Runtime Version.

2.2.2. Encrypt database communication

The communication between PONTON X/P and the database can only be encrypted if both support the encryption and if it is turned on. The required configuration depends on the used database driver in the Messenger. The configuration can be changed with the PONTON X/P GUI as follows:

Go to the database settings in MESSENGER > Settings and configure the database URL accordingly:

- Database URL for Oracle (Oracle Database JDBC Driver)
  - jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=servername)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=servicename)))
  - You find further details here: https://docs.oracle.com/en/database/oracle/oracle-database/19/jjdbc/client-side-security.html
- Database URL for MS SQL Server (Microsoft JDBC Driver)
  - jdbc:sqlserver://serverhost:1433;databaseName=AdventureWorks;encrypt=true;trustServerCertificate=true
  - You find further details here: https://docs.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption
- Database URL for MySQL (MySQL Connector/J)
  - jdbc:mysql://serverhost:3306/database?useSSL=true
  - You find further details here: https://dev.mysql.com/doc/connector-j/en/connector-j-reference-using-ssl.html

2.2.3. Strict SSL check when sending messages

In the messenger default configuration the issuer certificate is not checked when transmitting messages. You can activate that in the PONTON X/P GUI as follows:

1. Go to Messenger > Settings > General Settings and select the accordion tab > Communication
2. Enable “SSL Server Certificate check” with the checkbox
3. Click on „Save settings“ in the top bar
4. Stop and Start the Messenger

2.2.4. Replace default SSL certificate in Listener

Listener certificates can be changed under LISTENER> LISTENER CERTIFICATES in the PONTON X/P GUI. Please follow the following steps, a manual restart of the Listener is not required.

1. Got to Server Certificates tab
2. Check if the following subject of the certificate is there: "CN=localhost"
3. If yes, a new corresponding certificate must be requested
4. Click on request certificate
5. Please enter the entire domain-name or public IP of the Listener in the filed "SAN Value" and in the field “Certificate name”
6. Once you have filled out the other fields click on request certificate
7. Copy the certificate request and raise a CSR support ticket in PONTONs Service Desk
8. Before you install the SSL Server Certificate check "Update CA certificate" below
9. Install SSL Server Certificate

2.2.5. Disable weak TLS-ciphers in the Listener

Weak TLS encryption in the Listener can be switched of as follows:

1. In the installation directory of the Listener you find in the /config folder the file “Listener.properties”
2. Open the file in a text editor
3. Replace the code line „SSLDisabledCiphers“ with the following code line:
4. „SSLDisabledCiphers = **EXPORT**,**anon**,**DES**,**_DH**,**NULL**,*SHA“
5. Save the file
6. Stop and start the Listener

2.2.6. Update CA certificate

Versions 3.7.0 and below of the PONTON XP Messengers und Listeners were distributed with a PONTON Root CA certificate that is now outdated. This certificate must be replaced with the latest PONTON Root CA certificate:

PONTON Root CA Certificate

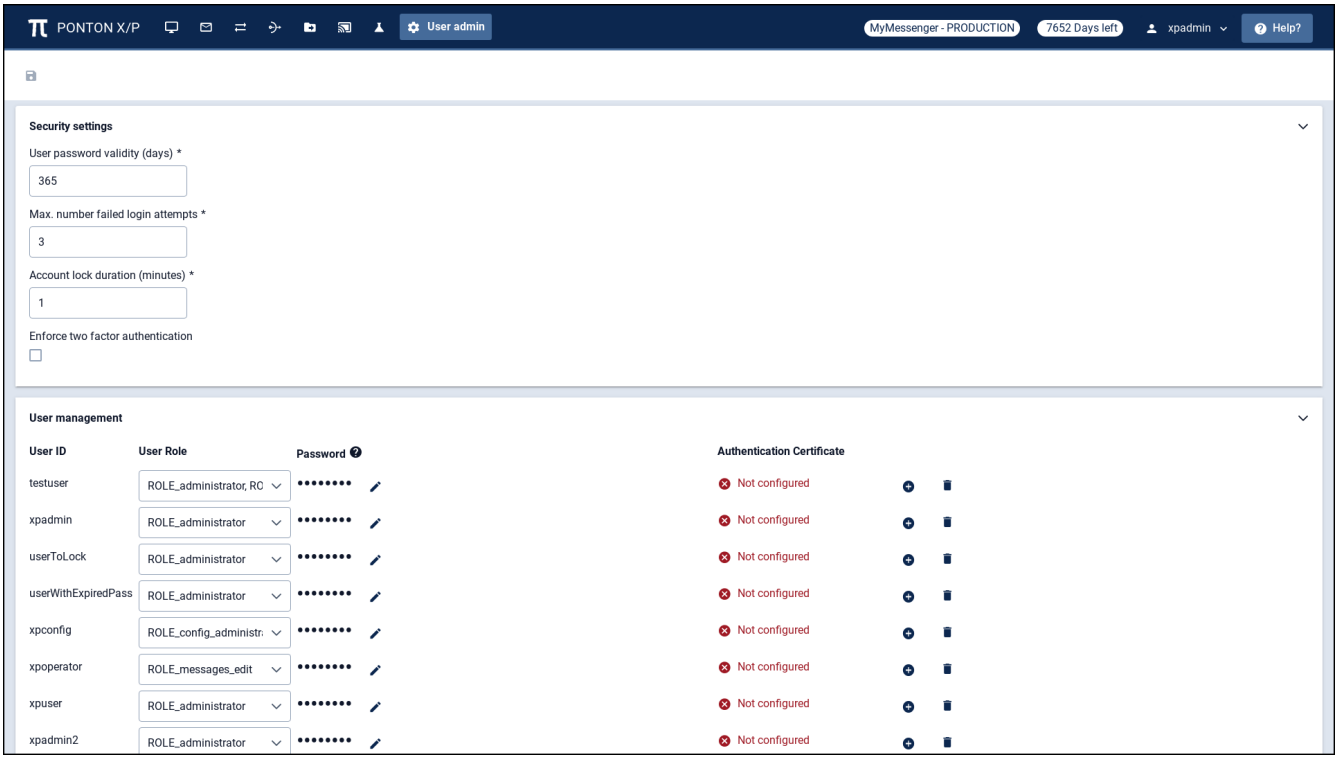
```
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIJAK46AzQ+zY+NMA0GCSqGSIb3DQEBCwUAMIGdMQswCQYD
VQQGEwJERTEQMA4GA1UEBxMHSGFtYnVyZzEfMB0GA1UEChMWUG9udG9uIENvbnN1
bHRpbmcgR21iSDEYMBYGA1UECxMPTmV0d29yayBTZXJ2aWNlMRcwFQYDVQQDEw5Q
b250b24gUm9vdCBDQTEoMCYGCSqGSIb3DQEJARYZaW5mb0Bwb250b24tY29uc3Vs
dGluZy5kZTAeFw0xMzA5MTcxMjMzMzhaFw00MzA5MTAxMjMzMzhaMIGdMQswCQYD
VQQGEwJERTEQMA4GA1UEBxMHSGFtYnVyZzEfMB0GA1UEChMWUG9udG9uIENvbnN1
bHRpbmcgR21iSDEYMBYGA1UECxMPTmV0d29yayBTZXJ2aWNlMRcwFQYDVQQDEw5Q
b250b24gUm9vdCBDQTEoMCYGCSqGSIb3DQEJARYZaW5mb0Bwb250b24tY29uc3Vs
dGluZy5kZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMcXG30x4Whw
WIoKZAEycUXMd0Q8vYrWWhfgvD4kH4eyIyZ8AStkd8cMHDqkYJAszPL0pFwIPEM0
bGcxgCNcUvzWlsyc9Ia7gv7cV6lpG/HFO6fk5jH9phKsJnvKHHWf/WuIb5j/KlVR
pQ/3wRuVD1zNSs4J25eAHzO2I5xMvVaUJoNU71WFsBNwPF39YKFZWnjpgxSaQPFE
dba+xi55vQzIPq+7ZMsEth736pqQXRym3hSkftYmstdPbNVAuOXHabOe92qrr84l
bevURoVtBXCUbRX+n09aEbw6jufRWQEz9TCEG0l/JWoQonaWvNEi9N/V8bsvQvqS
hk3VyhTE8P8CAwEAAaNzMHEwCwYDVR0PBAQDAgEGMA8GA1UdEwQIMAYBAf8CAQAw
HQYDVR0OBBYEFDPyUbiXrsoLT6TA3+pJNns3wzErMB8GA1UdIwQYMBaAFDPyUbiX
rsoLT6TA3+pJNns3wzErMBEGCWCGSAGG+EIBAQQEAwIABzANBgkqhkiG9w0BAQsF
AAOCAQEAOaKRf5yxLiHPWpFqWUS1E6tP1kBFY4OKKG6omRUgruf9h+AqWYlpn4QP
qd1hS6OnGOcHjgw8F4dDFcmO3IYcGwdpF+2KFmVJB5NNYHja9PFN7rX2tooSyRNj
T3bHyFVnWWeT58U2uqBO6y/S1qEErppBbFPZcfGS8eSQ+F3cz8b05QG5RQYTup6V
Wk+fHSccyO5b05gAhKVdhpAh0ebpfSpyko19f2mcPRZ2WAJyzmthzqHtunlN8zf1
ONLmM809tsr5qOhh4gnILlf8cuNKNCo671YBVD5MYpWq7rO4PO58vm03cvPszkHL
cO5Ms+BvYqg14GLDxMeoa72aa9/t6w==
-----END CERTIFICATE-----
```

Please follow the following procedure in order to update the PONTON Root CA Certificate:

1. Go to LISTENER > LISTENER CERTIFICATES in the PONTON X/P GUI
2. Select „Install CA certificate“ and install the certificate shown above
3. You will receive an error Message as the old certificate will be overwritten
4. Enable checkbox “Overwrite certificate” and save again
5. Go to “Client Certificates” and repeat installation steps
6. Go to MESSENGER > SETTINGS
7. Select “Server Certificate” and repeat installation steps

3. User Admin

Go to: **USER ADMIN** ⚙



3.1. Enter and change security settings

3.1.1. Change user password validity

The expiry period for new user passwords is set by default to 365 days. To change this value please enter the new value (days) in the "**User password validity**" field and click on the save 💾 icon. The value must be between 0 and 365 days and you can't leave the field empty. With a value of 0 there will be no password expiry.

3.1.2. Change number of failed login attempts

A user account is temporarily locked when the number of failed login attempts exceeds a defined number. The default value for the maximum number of failed login attempts is 3. Enter the new number of failed attempts in the "**Max. number failed login attempts**" field and click on the save 💾 icon. You can't leave the field empty.

3.1.3. Change account lock duration

The duration of the temporary lock to prevent brute force attacks can also be adjusted. By default accounts are locked for 1 minute. Enter the new lock duration in minutes in the "**Account lock duration**" field and click on the save 💾 icon. You can't leave the field empty.

> [Info Icon] **Unlock account**
> It is possible to unlock an account by using an administrator account to reset the password of

a locked account.

3.2. User Management

3.2.1. Create a new user

When you click on the "*Create new user*" + icon, a new row of input fields is added to the user settings table. Enter a **User ID** in the "*USER ID*" field and select a User role with the drop-down menu.

The following (pre-defined) user roles are available as **default** to choose from:

- **ROLE_administrator** – these users have full access to the Messenger's configuration interface (REST API).
- **ROLE_config_administrator** – these users have the same rights as Administrators but can not create new user or change user settings.
- **ROLE_operator** – these users are not allowed to make changes to the configuration, however they can view the current configuration.
- **ROLE_httpadapter -** API users with full access to the HttpAdapter endpoints.
- Additionally, there is a pre-defined **ROLE for each page and/or tab** available (to view and edit) in the messenger UI to choose from, such as:
  - ROLE_settings_view
  - ROLE_messages_edit
  - ROLE_partner_edit
  - etc.

[Info Icon] Certain pre-defined roles automatically enable the user to view and edit other iterrelated pages as well.

It is also possible to define customized roles in the messenger. For this purpose please refer to the section 'Roles Management' for details.

Please enter a valid password as well as repeat password for the new user. The new and repeat password must match and must meet the password criteria. You can view the password you have entered by clicking on the symbol 👁 or hide it by clicking on the symbol 🙈.

The password criteria are as follows:

- minimal length of 12 characters
- at least one UPPER case letter
- at least one lower case letter
- at least one number
- at least one special character (!\"#$%&'()*+,-./:;<⇒?@[]^_`\{|}´)

When you have entered all required details please click on the save icon.

3.2.2. Delete a user

Click on the delete icon on the right hand side next to the user you wish to delete. A confirmation dialog opens. Clicking on the "*Yes*" button will delete the selected user and the row will disappear from the table. Clicking on the "*No*" button will close the dialog and not delete the user.

3.2.3. Change user role

Click on the drop-down menu of the user you want to change and select the new role. Click on the save icon.

3.2.4. Edit user password

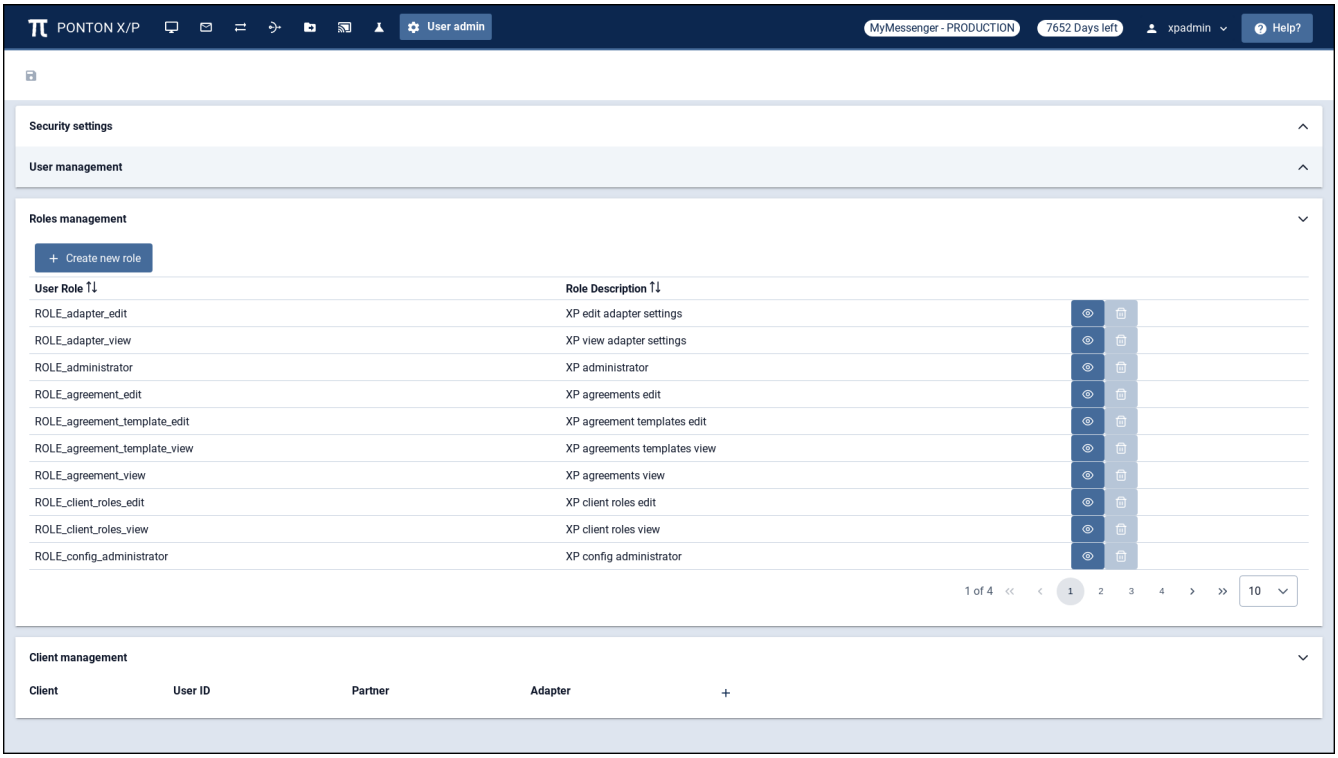
Click on the edit icon of the user which password you want to change. Enter a new valid password and matching repeat password. The password criteria are mentioned above (Create a new user). You can view the password you have entered by clicking on the symbol or hide it by clicking on the symbol . Click on the save icon. In case you decide to leave the password unchanged click on the **x** icon and discard the changes.

3.2.5. Authentication certificate

As an alternative to the user/password based authentication It is possible to use TLS certificates when connecting to the REST API. A certificate is directly linked to a user and its roles. Click on the add icon in the row of a user where a certificate should be linked, to upload a certificate. A restart of the Messenger is needed for the certificate authentication to work.

3.3. Roles Management

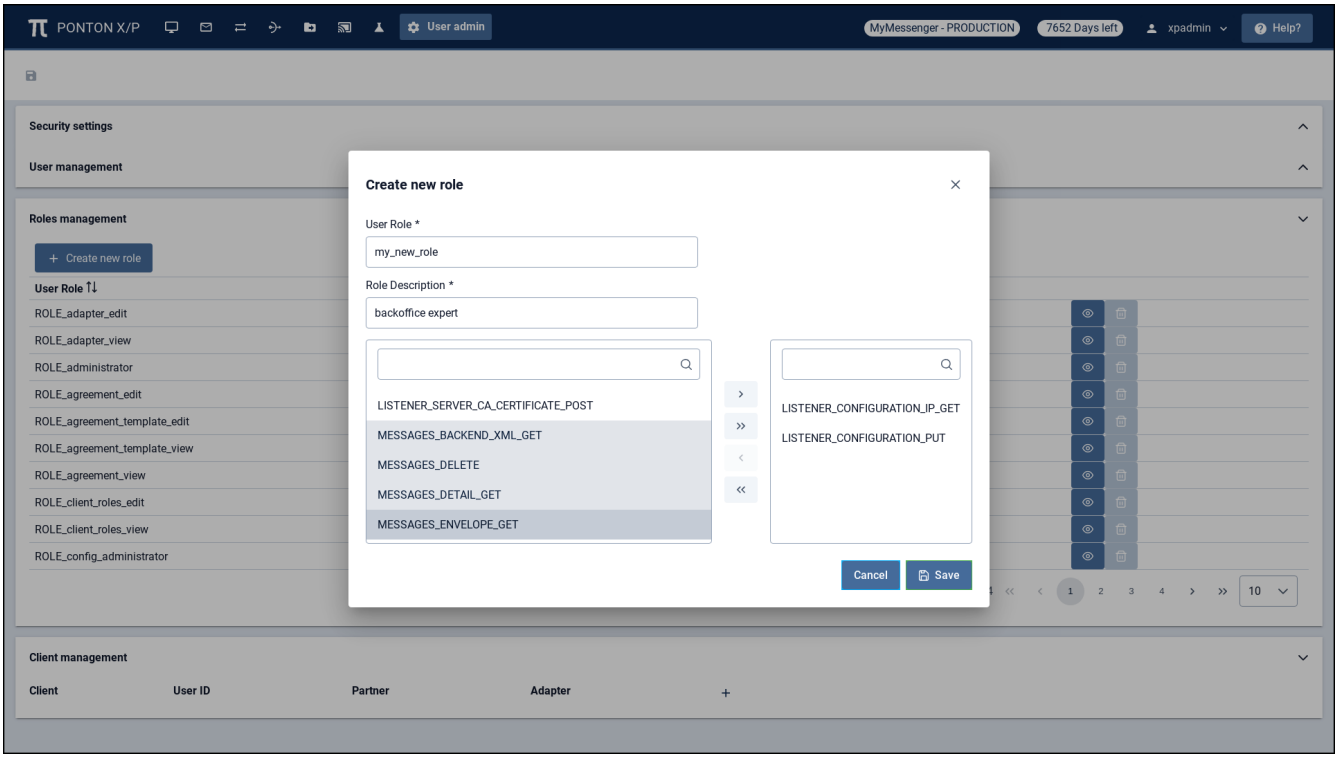
If the default roles provided with the messenger version do not exactly match your company's requirements then it is recommended to define new roles under User admin as follows. Click on the 'Create new role' button within the Role management section:



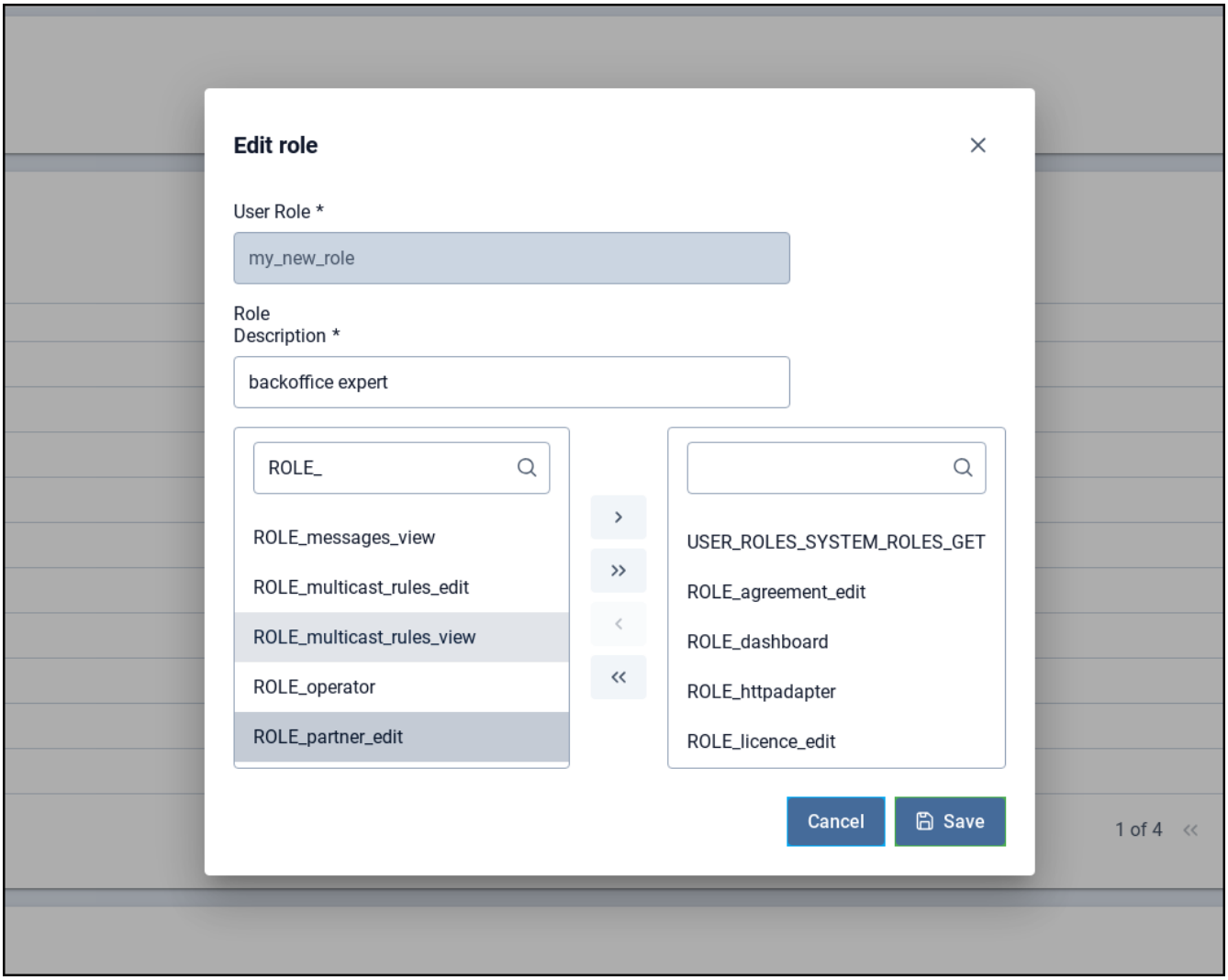
This will lead to a pop-up where you can define your required role.

1. Enter an appropriate and unique name as well as description for the new role.
2. Select from the list of available rights. The list of rights contains multiple entries since there is an entry available for each individual action which can be performed in the messenger UI. [Info Icon] For convenience purpose you can filter the list of available rights to choose from.
3. Click on › the symbol.
4. Remove the text from the filter field.
5. Save the changes.

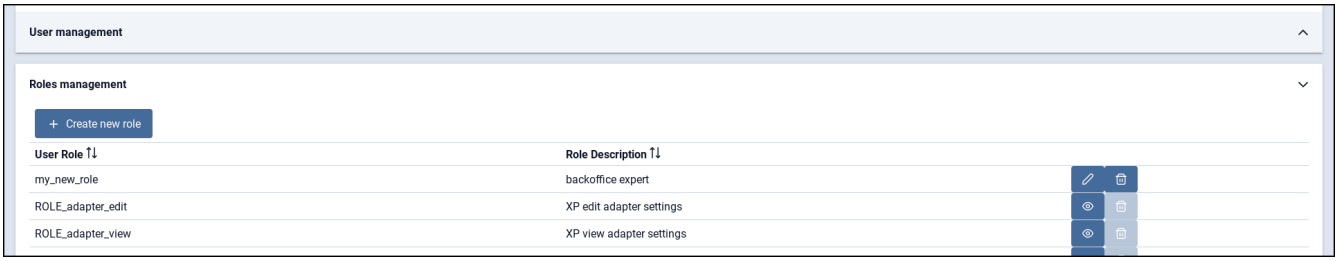
Hint: In case details are required for the available rights, it can be helpful to navigate to the documentation of the REST API, since these rights correspond to technical endpoints of this API which can be found at http(s)://<messenger_host>:<rest_port>/api/swagger-u



[Info Icon] While selecting the required rights from the list of available rights, it can be highly useful to filter for rights beginning with **ROLE_.**
This will show you a list of rights which correspond to the individual pages and tabs available in the messenger UI.



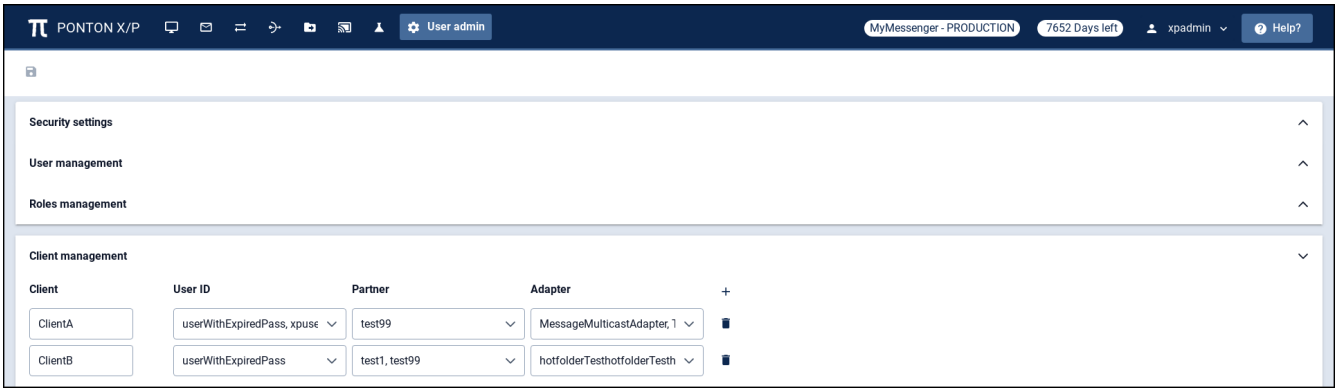
The newly created role is now shown in the table of roles and can be editied (✎) and/or deleted (🗑) as required.



3.4. Client Management

As service providers it is possible to set up access to the X/P messenger individually for each client. Users of each client are granted access limited to the (local) partners and adapters assigned to them.

[Info Icon] Users which are not assigned to clients have unrestricted access as far as partners and adapters are concerned.



Administrator (or users with the right to manage clients) can create a new client by clicking the + icon in the 'client management' section. The following inputs are required to create or edit a client before saving the changes by clicking on the 🖫 icon:

- **Client**: Name of the organisation or department.
  - [Info Icon] This name must be unique.
- **User ID**: Select one or more users from the available drop down list
  - Please ensure that the selected users have only the required rights and permissions by verifying that they have been assigned the correct roles as per these requirements!
    - ⚠️ It is recommended, that the assigned users shall not be granted the privilege of editing settings, users or roles, since, they can then see (and edit) user information of other clients.
  - [Info Icon] In case you wish to use a freshly created user, you might be required to refresh the settings page first.
- **Partner**: Select one or more partners from the available drop down list.
  - [Info Icon] This list only contains local partners. Thereby restricting the access of the

respective client users to messages and configuration which include these selected partners.

- **Adapter**: Select one or more adapters from the available drop down list.
  - [Info Icon] As a consequence of this selection only the selected adapters are allowed while creating or editing agreements or sending messages as a user of this client.

The newly created client is now shown in the list of clients and can be deleted (🗑) as required.

> [Info Icon] **Visible Adapters**
>
> If an adapter has been configured in agreements involving the partners of a client, then the Adapters are visible to the client user in the agreements table even though the Adapter has not been allocated to that particular client

4. Graphical User Interface Quick Starter

Please find below a simple guidance on how to use the PONTON X/P User Interface.

4.1. Find your way around

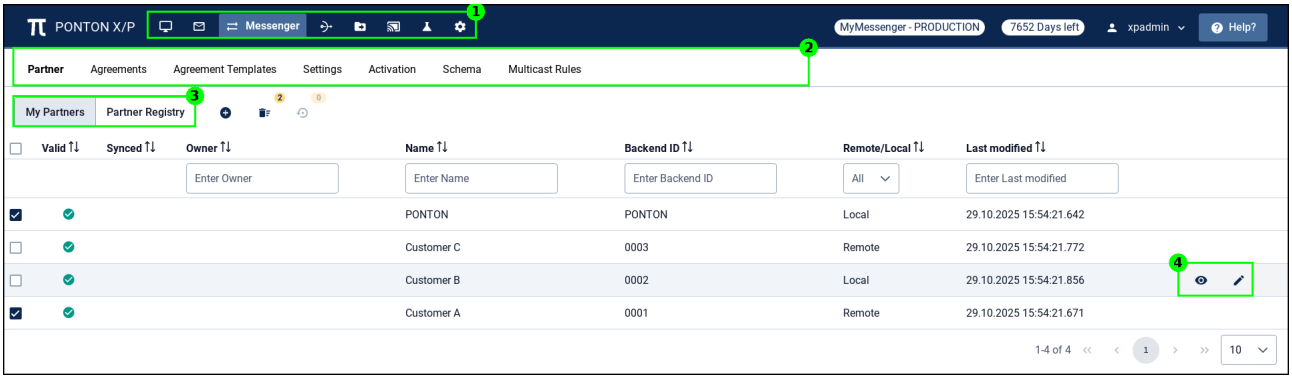
Navigating through the PONTON X/P Messenger is easy. The following navigation overview is helping you to quickly get you where you want to be and always ensures that you know where you are in the application.

1 **Main Navigation bar:** Enables you to navigate through the main functional areas of the PONTON X/P Messenger such as **Monitor**, **Messages**, **Messenger**, **Listener**, **Hotfolder**, **Http Adapter**, **Test Adapter** and **User Admin**.

2 **Sub-menu bar:** Enables you to find subordinate segments of the main areas e.g. Messenger, which is separated into **Partner**, **Agreements**, **Agreements Templates**, **Settings**, **Activation, Schema and Multicast Rules**.

3 **Tabs:** Enables you to toggle between separated parts of a coherent functional application.

4 **Quick Action Bar**: When you hoover with your mouse over items in the table the quick action bar will appear, enabling you to view or edit the selected item.

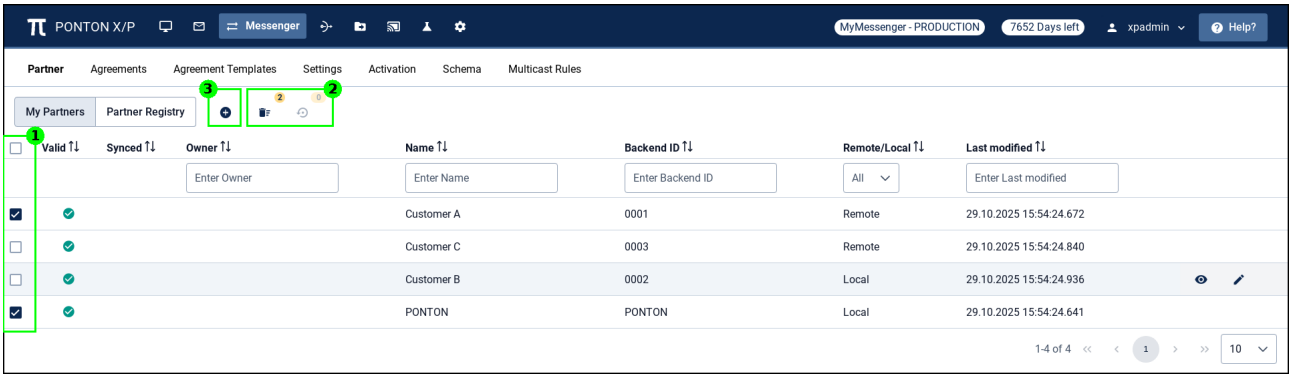


4.2. Select and execute actions

1 **Select Table Row(s):** Click on the checkbox to select or deselect the item (e.g. Partner, Agreement) you want to process. The number of selected item, which are actionable, is displayed next to the action icon.

2 **Toolbar:** When you have selected at least one actionable item you can click on the available action icon to execute the command. An icon tool-tip provides you with a hint about the underlying action.

3 **Create:** In order to create new **Partners (Local and Remote**), **Agreements** and **Hotfolder Adapters** click on the + icon in the action bar.

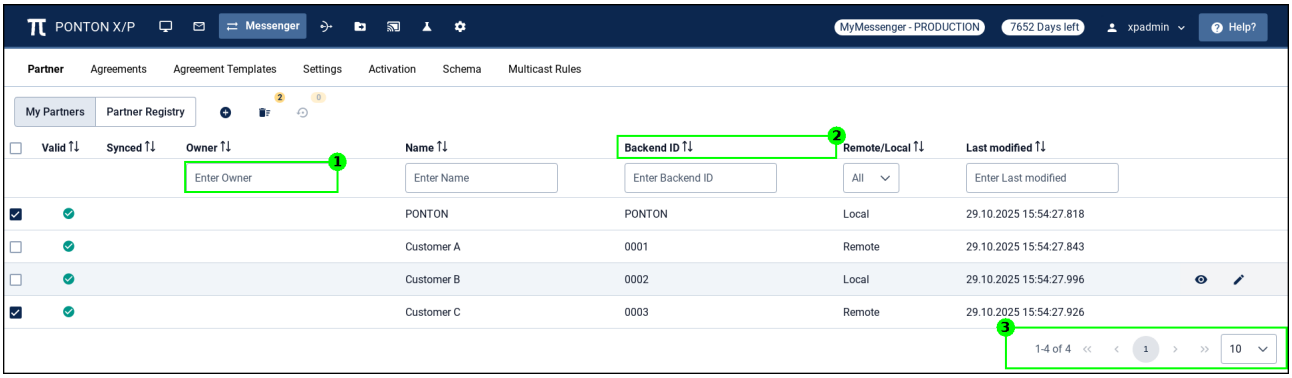


4.3. Arrange your data

1 **Filter:** Some table headings have a filter functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.

2 **Sorting:** All table headings have a sort function. You can sort ascending and descending.

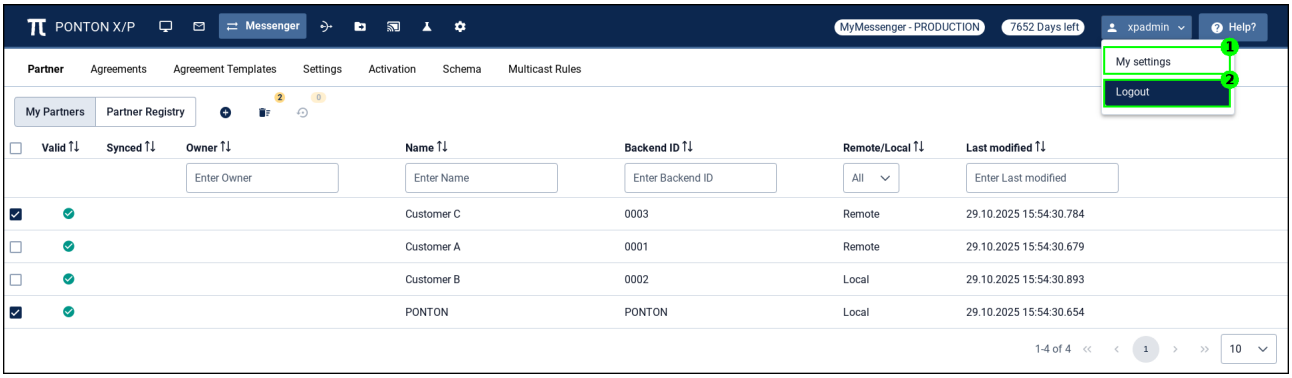
3 **Pagination:** The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.



4.4. Change your settings and log-out

1 **Change your settings:** Change your language settings and password.

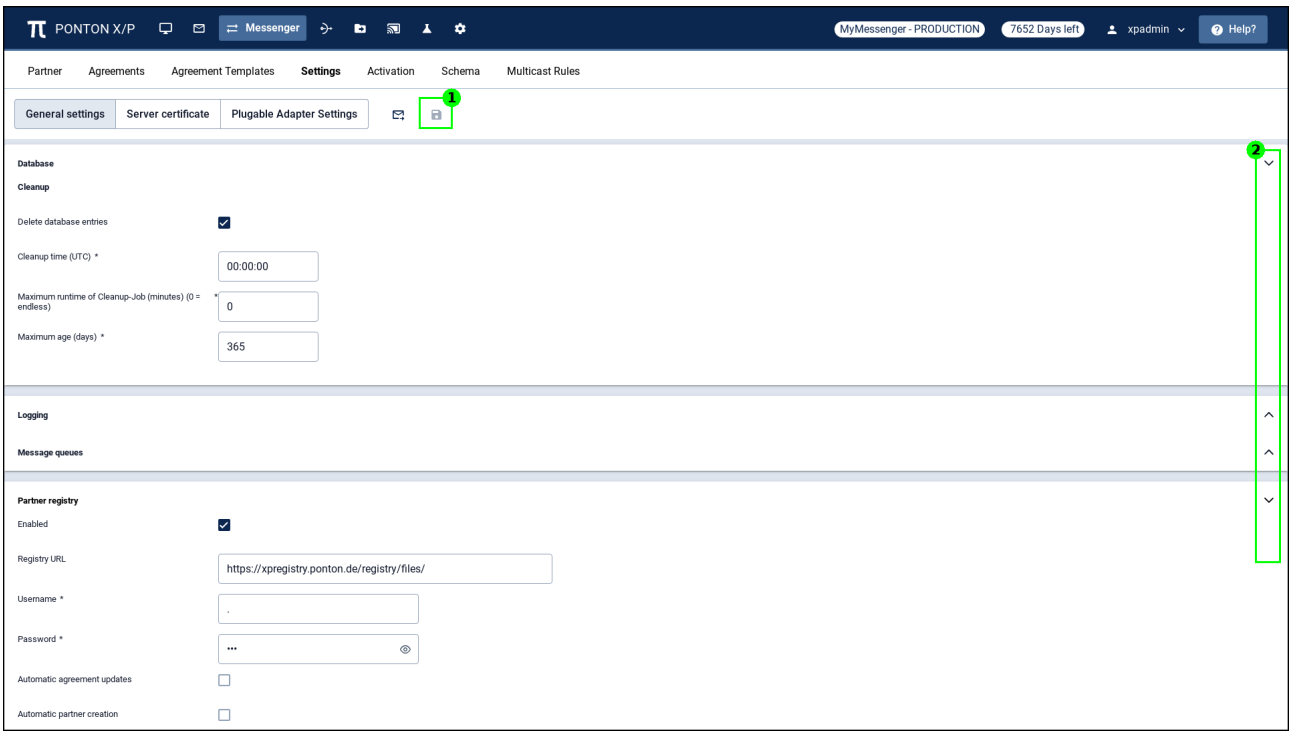
2 **Log-out:**



4.5. Configure settings

1 **Configure:** Open a configuration page (**Partner, Agreements, Agreements Templates, Listener, Hotfolder, Messenger Settings**), make the required changes by using drop-down menus, check-boxes, input fields etc. and click on save icon.

2 **Hide/unhide:** Use the accordion tabs to organize the layout.

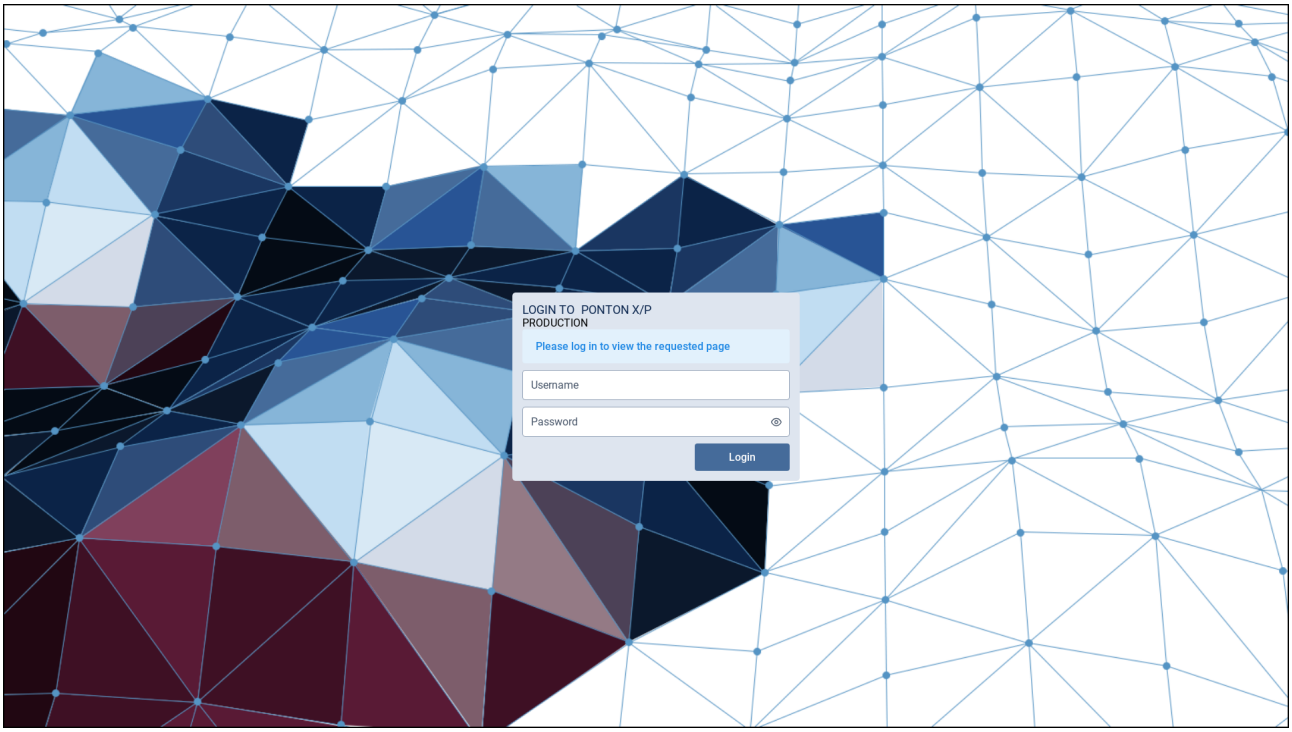


5. Main Navigation

5.1. Log-in

Please enter your username and password for logging-in to PONTON X/P. You can view the entered password by clicking on the view symbol 👁.

> ⚠️ **Failed login**
>
> If your login attempt failed you will not get any feedback why it failed. You will also not receive a notification that your account has been blocked due to too many failed attempts. This is best practice with regards to security.



5.2. Main Navigation (left)

Area	Symbol	Description	Subnavigation	Description
Monitor	🖵		• Dashboard	
			• Adapter Status	
Messages	✉	View Messages and its details, Resend and Delete Messages		

Area	Symbol	Description	Subnavigation	Description
Messenger			• Partner	Create and edit own / communication Partner; Add and manage Partner Certificates
			• Agreements	Add, configure, delete Agreements
			• Settings	Configure general Messenger settings; Manage Server Certificate
			• Activation	Get license info; Send activation requests; Install activation and license
			• Schema	Install or update SchemaSets
			• Multicast Rules	Define Rules for Message duplication
Listener		Remote configuration of the connected Listener; Manage Listener Certificate and Client certificates		
Hotfolder		Add, configure, delete Hotfolder		
Test Adapter		Send test Messages; Ping receiver		
User Admin		Manage user accounts		

5.3. Main Navigation (right)

5.3.1. Set Messenger instance name

On the navigation bar you see the **Messenger Instance Name** which can be changed to display a name that easily identifies the system. It is configured on the Messenger >Settings page.

Further you see how many days are left until the license expires as well as the user name of the user who is logged-in.

Area	Symbol	Description	Sub-Navigation	Description
User Menu			• User Settings	Change your language settings and your password

Area	Symbol	Description	Sub-Navigation	Description
			• Logout	Log out of PONTON X/P
Help?			• Manuals and release notes links	
			• Support Portal (external link)	Go to PONTON X/P support website
			• Product Page (external link)	Go to PONTON X/P product website
			• UI-3rd party licenses	list all 3rd party libraries used for the UI and their licenses
			• Java-3rd party licenses	list all 3rd party libraries used for the Java backend and their licenses

5.4. User Menu

5.4.1. Change your language settings

Click on the  username icon so that the user menu drop-down opens and select "*User Settings*". Select the language you want from the drop-down menu. Click on the "*Save Settings*" button which becomes active when you have selected a new language.

> [Info Icon] **Browser default language**
>
> When you select "browser default language" and PONTON X/P does not support your browser default language it will select English as default language.

5.4.2. Change your password

Click on the  username icon so that the user menu drop-down opens and select "*User Settings*". Type in your current password as well as the new password and repeat password. The new and repeat password must match and meet the password criteria. You can view the password you have entered by clicking on the symbol  or hide it by clicking on the symbol  . The password criteria are as follows:

- minimal length of 12 characters
- at least one upper case letter
- at least one lower case letter
- at least one number
- at least one special character

When you have entered all three passwords, and they are valid and matching, the "*Save Password*" button becomes active.

5.4.3. Log-out

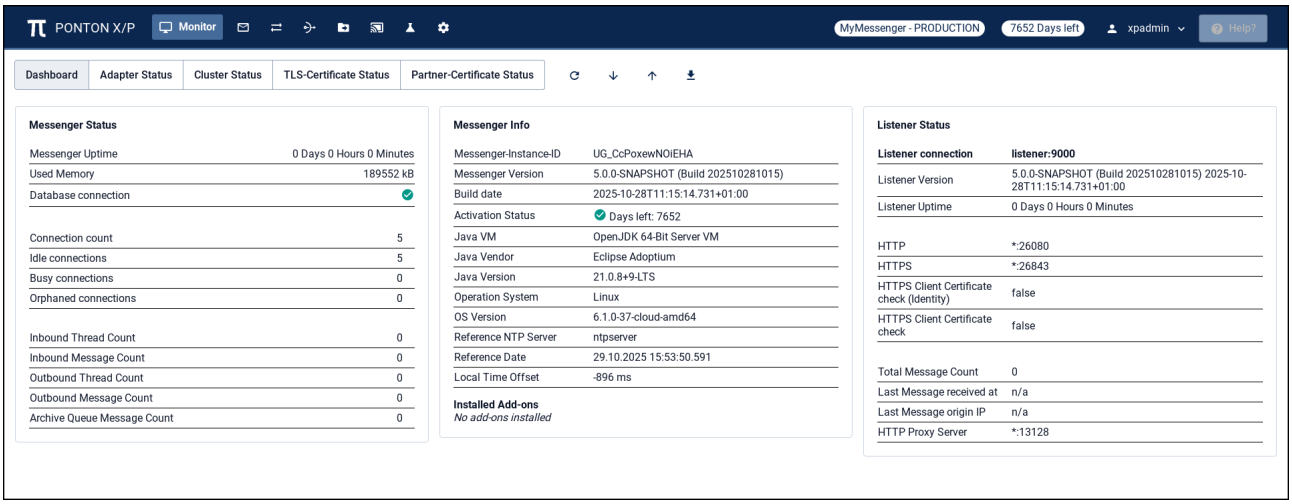
Click on the person username expand_more icon so that the user menu drop-down opens and click on the "*Log-out*" button.

6. Monitor

6.1. Dashboard

Go to: **MONITOR** > **Dashboard**

After logging in to the PONTON XP Messenger the Monitor Dashboard screen is displayed. The Monitor Dashboard is showing information about the current server configuration and the status of different Messenger processes (Threads). You can always navigate back to the Monitor Dashboard by clicking on the **Monitor** icon on the navigation bar.



6.1.1. Restart Messenger

In case you want to restart the Messenger click on the restart icon. You need to confirm the restart. While the Messenger is restarted the connection to the server is lost and the PONTON X/P Messenger can not be used. The database connection symbol is displaying a symbol and there is no other status information visible on the Dashboard. When the server connection is established again, the database connection symbol is displaying a symbol and the PONTON X/P Messenger can be used again.

6.1.2. Download config files

Click on the download config files icon to download the config of the messenger. The download contains the configuration data from the filesystem as well as the database.

6.1.3. Upload config files

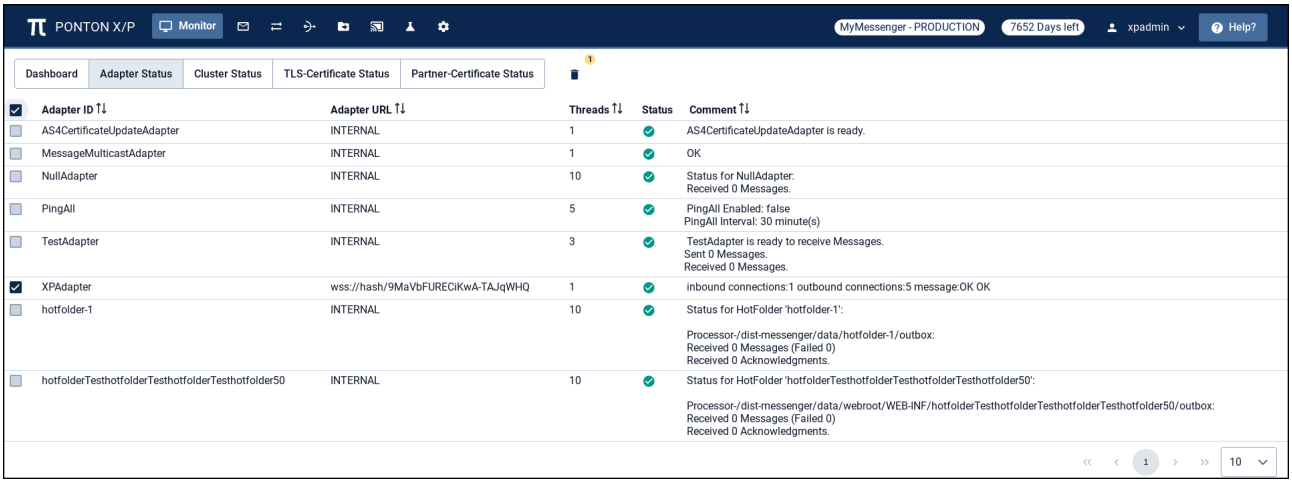
Click on the upload config files icon to upload the config downloaded before. The uploaded config will be merged with existing configuration. This means existing config entries matching with uploaded ones, will be overwritten. New config entries from upload will be added. All other config entries shall remain unmodified by the upload.

6.1.4. Download log files

Click on the download log files icon to download the log files to a download folder in your local system.

6.2. Adapter Status

Go to: **MONITOR** > **Adapter Status**



An overview of the adapters connected with the PONTON X/P Messenger can be obtained by clicking on the "**Adapter Status**" tab next to the Dashboard tab. If the symbol in the status column is showing a check mark symbol which means that the adapter is working and accepting messages.

All table heading have a **Sort** function (icon). Sort can be ascending and descending. Underneath the table in the bottom right corner you find a **Pagination**. function The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward pages by clicking on the page number, the forward backward icons or the first page last page icon. The active page is highlighted in blue.

> [Info Icon] **Adapters**
>
> Adapters running as embedded adapters are shown with an adapter URL as INTERNAL, these adapters cannot be deleted. Depending on the adapter type, there will be additional status information in the comment column.

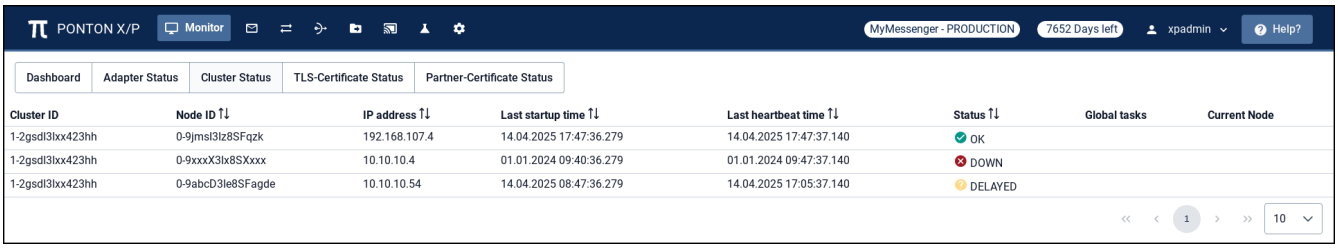
6.2.1. Delete Adapter reference(s)

If an external adapter is no longer required, then the Adapter reference can be deleted manually. To delete Adapter reference(s) select the Adapter reference you want to delete with the checkbox on the left hand side of the table row. With the checkbox in the headings row you can select all Adapters. The number of selected Adapters is displayed above the delete icon. Click on the delete icon and confirm that you want to delete the selected Adapter references. When clicking on the "*OK*" button on the confirmation dialog, the Adapters will no longer be displayed in the table.

[Info Icon] Adapters using the adapter API 2.0 will be shown with an adapter URL using websocket (wss) as protocol. Authorization of an adapter connected via API 2.0 is performed using the instance ID at the end of the adapter URL.

6.3. Cluster Status

Go to: **MONITOR** > **Cluster Status**



This page shows the status of Messenger nodes of the cluster. For each node the following details are shown:

- Cluster ID: unique identifier for the cluster setup
- Node ID: unique identifier for each cluster node
- IP address: the IP address of each cluster node
- Last startup time: the time when the cluster node was started
- Last heartbeat time: Each cluster node sends a periodic "heartbeat".
- Status: This is based on the heartbeat
  - OK, if heartbeat was received less than 1 minute ago
  - DELAYED, if heartbeat was received between 1 - 3 minutes
  - DOWN, if heartbeat was received more than 3 minutes ago
- Global tasks: indicates which cluster node is currently executing global tasks (e.g. database cleanup, archive cleanup, etc.)
- Current Node: indicates which cluster node you are currently connected to

6.4. TLS Certificate Status

Go to: **MONITOR** > **TLS-Certificate Status**

On this page you can see an overview of all known remote server certificates. You can delete selected certificates or export them.

The following details are shown:

- status of the certificate shows the validity of the certificate
  - valid
  - expired

    - ⚠ nearly_expired (will expire within two weeks)
    - ✖ revoked
    - ✖ temporarily_disabled (recovation status could not be checked for more than 3 days)
- certificate subject
- certificate issuer
- certificate key-algorithm
- certificate serial number
- certificate validFrom and validTo
- certificate's last validity check
- revocation reason

6.5. Partner Certificate Status

Go to: **MONITOR** 🖵 > **Partner Certificate Status**

On this page you can see an overview of all partner certificates. You can delete selected certificates, export them or navigate to the corresponding partner.

The following details are shown:

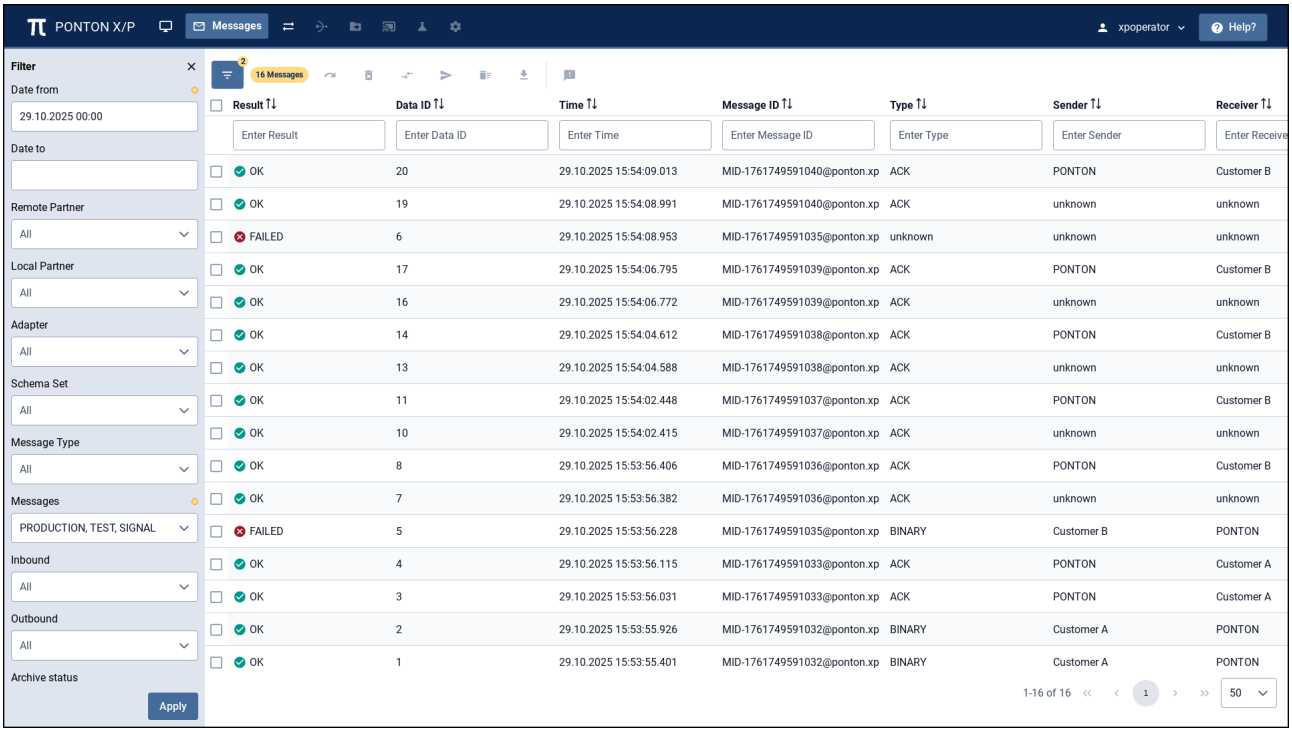
- status of the certificate shows the validity of the certificate
    - ✔ valid
    - ✖ expired
    - ⚠ nearly_expired (will expire within two weeks)
    - ✖ revoked
- certificate subject
- certificate issuer
- certificate key-algorithm
- certificate serial number
- certificate validFrom and validTo
- partner display name

7. Message Monitor

Go to: *MESSAGES *

Messages sent and/or received by your Messenger can be viewed and filtered with the Message monitor.

[Info Icon] In case User Admin#Client Management is active only those local partners and adapters will be provided which are relevant for the active user.



7.1. Filter Messages

7.1.1. Select filter criteria

A date picker with date/month/year and hour/minutes is available for the following criteria:

- **From** - filter messages created after the entered 'from' time (local server time), default filter setting: today-1 00:00
- **To** - filter messages created before the entered 'to' time

A multi-select drop-down-list with search function (type in filter value into search text field above the drop-down-menu) is available for the following filter criteria:

- **Remote Partner** - involved communication partner
- *Local Partner *- involved own partner
- **Adapter** - involved adapter
- **Schema Set** - schemaset of the processed message
- **Message Type -** message code according to schemaset

- **Messages** - characteristic of the message (PRODUCTION, TEST or SIGNAL) with PRODUCTION as default filter setting.
- **Inbound** - state of the inbound message
- **Outbound** - state of the outbound message
- **Archive status** - archiving state of message

Active filter have a yellow dot next to filter indicating that the filter was selected. The Filter Badge shows the number of active filters.

7.1.2. Set further message filter attributes

An additional text filter is available for the following input fields:

> ⚠ **Like Search**
>
> Use '%' as wildcard symbol for a like search

- **Protocol Info** - protocol info of the processed message.
- **Message ID** - message ID of the processed message.
- **Conversation ID** - conversation ID of the processed message.

Click on the Toolbar filter icon in order to hide or show the filter bar. Alternatively you can close the filter bar by clicking on the **x** icon in the top right corner of the filter bar.

7.2. View Messages and trigger message Actions

Select your filter criteria and click on the "*Apply*" button to get all Messages which match the filter criteria in the Messages table. The number of messages which meet the filter criteria is displayed in the yellow badge next to the filter icon. The Messages table displays a list of all Messages. The filter results are ordered by message timestamp descending (newest first). Each time a search has been successfully finished the user receives a success message, indicating that the search was finished, even though no new entries were found.

> ⚠ **Records Found**
>
> As the amount of records can be very large with too wide filter settings, a fixed maximum number of records is returned with the filter (e.g 2000, this is configurable). The total number of found records is displayed (e.g. 2000 / 100.000 - which means 2000 messages were returned, but 100.000 were found with this filter criteria. Pagination and sorting in the GUI table is done within the initial result set. To retrieve a new set of records the filter criteria must be changed and applied by clicking on the "*Apply*" button again.

7.2.1. Table headings

- **Result** - Status of Message (OK, Failed, In Process, In Transit, Archived) with graphical representation with icon.
- **Data ID** - Technical unique ID of the processed message
- **Time** - Time when message was created in local server time
- **Message ID**- Message ID of the processed message
- **Type** - Message type according to schemaset
- **Sender** - Name of ID of sender
- **Receiver** - Name of ID of receiver
- **I/O** - Inbound or Outbound direction
- **Test** - Test messages = true
- **Adapter** - Adapter ID of the involved adapter
- **Protocol** - Protocol info of the processed message
- **Conversation ID** - Conversation ID of the processed message
- **Archive status** - Status of Archiving of Message (Ok, Failed, Unprocessed, In Process, Failed and rescheduled, Enqueued) with graphical representation with icon.
- **Loginfo** - Log Info of the processed message

The following functions are available to easily find the table entry in the Messages you are looking for:

- All table heading have a **Sort** function (icon). Sort can be ascending and descending.
- Some table Headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 50 entries per page and can be changed to 100, 500, 1000 or 2000. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.

7.2.2. Resend messages

Select the Messages you want to re-send by clicking on the checkbox ☐ on the left hand side of the Message table. The number of selected Messages is displayed next to the resend ↷ icon. When you click on the re-send ↷ icon, the process of re-sending the selected Messages is started and a progress window opens. During the process you can not use other functions of PONTON X/P GUI. You can stop the process at any time, but it will not affect Messages which have already been re-sent. The progress window displays the number of total Messages to be processed, already processed Messages and number of errors occurred. You can see details (Data ID and Message ID) of the errors by clicking on the > icon. When the process is finished (or you stopped it), you can click on the "*Close window*" button and continue using PONTON X/P GUI.

7.2.3. Delete messages

Select the Messages you want to delete from the database by clicking on the checkbox ☐ on the left hand side of the Message table. The number of selected Messages is displayed next to the delete icon. When you click on the delete icon a confirm dialog opens. Clicking on the "*OK*" button is starting the process of deleting the selected Messages and a progress window opens. During the process you can not use other functions of PONTON X/P GUI. You can stop the process at any time, but it will not affect Messages which have been already deleted. The progress window displays the number of total Messages to be processed, already processed Messages and number of errors occurred. You can see details (Data ID and Message ID) of errors by clicking on the > icon. When the process is finished (or you stopped it), you can click on the "*Close window*" button and continue using PONTON X/P GUI.

7.2.4. Delete messages from queue

Select the Messages with status "IN TRANSIT" you want to delete from the message queue by clicking on the checkbox ☐ on the left hand side of the Message table. The number of selected Messages is displayed next to the delete icon. When you click on the delete from queue icon a confirm dialog opens. Clicking on the "*OK*" button is starting the process of deleting the selected Messages and a progress window opens. During the process you can not use other functions of PONTON X/P GUI. You can stop the process at any time, but it will not affect Messages which have been already deleted. The progress window displays the number of total Messages to be processed, already processed Messages and number of errors occurred. You can see details (Data ID and Message ID) of errors by clicking on the > icon. When the process is finished (or you stopped it), you can click on the "*Close window*" button and continue using PONTON X/P GUI.

7.2.5. Send messages to new adapter

Select the Messages you want to send to a new Adapter by clicking on the checkbox ☐ on the left hand side of the Message table. The number of selected messages is displayed next to the send to new adapter icon. When you click on the send to new adapter icon a dialog box opens where you can select the Adapter to which you want to send the selected Messages. Select the Adapter and click on the "*Send*" button, which is starting the process of sending the selected Messages to a new Adapter and opens a progress window. During the process you can not use other functions of PONTON X/P GUI. You can stop the process at any time, but it will not affect Messages which have been already sent to a new Adapter. The progress window displays the number of total Messages to be processed, already processed Messages and number of errors occurred. You can see details (Data ID and Message ID) of errors by clicking on the > icon. When the process is finished (or you stopped it) you can click on the "*Close window*" button and continue using PONTON X/P GUI.

7.2.6. Resend all messages with bulk resend

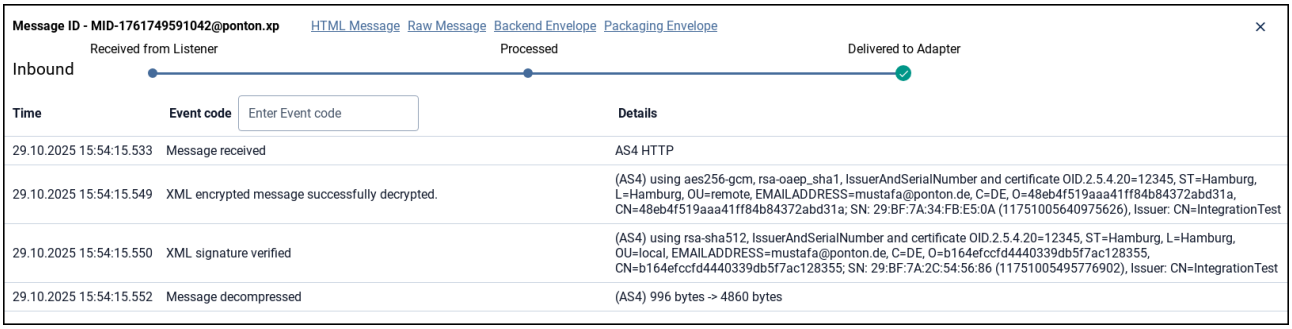
This function will resend either all inbound or outbound failed messages. You need enter a valid date in the "Date from" search field and select "FAILED" in the Outbound or Inbound selection of the filter bar before the icon becomes active. Selecting certain messages in the Message Monitor will not activate the button. When you have entered the above mentioned valid filter settings the number of failed Messages is displayed next to the bulk resend icon and the icon becomes active. When you click on the active bulk re-send icon a confirmation window will appear.

When you click on "Yes" the dialog closes and the re-sending process is starting. You can only start one bulk re-sending process at a time. Should you nevertheless try to start a new re-sending process when a process is already in progress you will get an error dialog: "Request denied. There is already a re-transmission process in progress."

7.2.7. Toggle between failed and resolved status of messages

Select the FAILED (or resolved) Messages you want to change status by clicking on the checkbox ☐ on the left hand side of the Message table. The number of selected Messages is displayed next to the "Toggle Message Status" icon ⇢←. When you click on the "Toggle Message Status" ⇢←, a confirm dialog opens. Clicking on the "*OK*" button is starting the process of changing the status of all selected Messages from FAILED to RESOLVED or vice versa.

7.2.8. View details of a message



You can view details of every Message displayed in the Message table. When you hoover with your mouse over the Message table, a view 👁 icon will appear for each Message. Click on the view icon 👁of the Message which details you want to view and a detailed list of events will be shown for the chosen Message in the bottom half of the message screen. You can close the detailed view by clicking on the **x** symbol in the top right corner of the detailed view window.

The **Message ID** of the selected Message and the current processing step and process/transfer status of the Message is displayed in the graph. If the transfer was successful a green check-mark ✅ symbol is displayed, if something went wrong a red cross symbol ❌ is displayed.

Next to the Message ID you may find one or download links in various formats for the selected Message ID. The following formats might be available:

- **HTML Message** - get the message content in HTML format generated by the messenger
- **Raw Message** - get the original message content
- **Backend Envelope** - get Backend Envelope as a list of key value or as XML depend of involved adapter
- **Packaging Envelope** - get Packaging Envelope as a text or as XML depend of used packaging

When you click on one of the links mentioned above, the Message will be downloaded to a folder in your local directory in the selected format.

In the table below the status graph you can view the following details for the Message ID.

- **Time** - time of the created message event (displayed as local server time)

- **Event code** - description the occured message event
- **Details** - additional description the occured message event

7.2.9. Add or change the log info of a message

When you hoover with your mouse over the Message table, an "Edit log" will appear for each Message. Click on the "Edit log" icon the Message which logs you want to edit and a modal dialog will appear. Enter the log info and click on "Save". Please note that log info dialog is a free text field with max. of 128 characters. If you don’t want to save the changes click on "Cancel". The Log info is now displayed in the Message Monitor table.

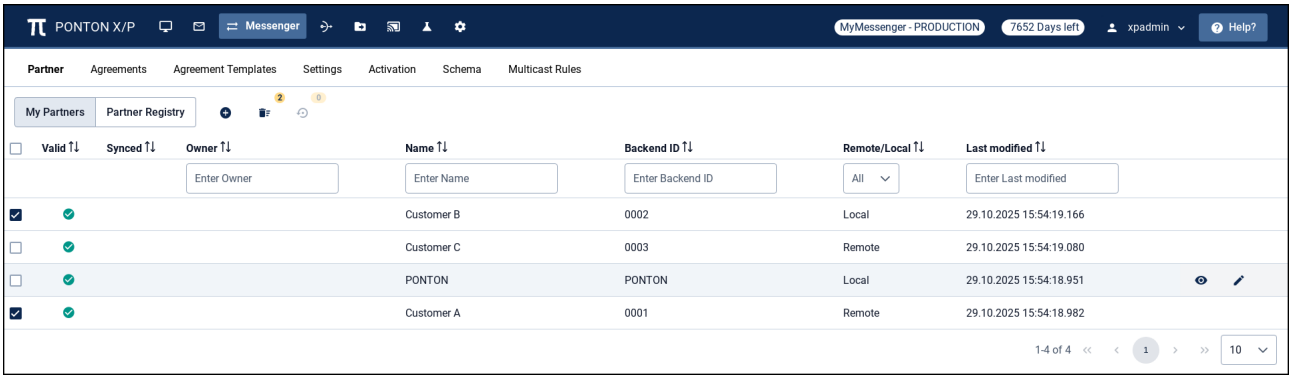
8. Messenger >Partner

A Partner profile can be seen as representing the communication capability of the respective Partner. A Partner may, for example, support HTTP(S), SMTP, SMIME and FTP(S) as transport protocols. An Agreement (see **Agreements**) between two Partners restricts the capabilities of two Partners to a choice of options that are supported by both sides. In the case of the transport protocol, the partners might define HTTP as the protocol they want to use.

[Info Icon] PONTON X/P distinguishes between **Local** and **Remote** partners – this distinction indicates whether the partner refers to a local partner within your own PONTON X/P system or to a communication partner on an external system. The configuration steps might differ slightly. For example, you can submit a certificate request for a Local Partner, but not for a Remote Partner.

8.1. My Partners

Go to: **MESSENGER** ⇄ > **Partner** > **My Partner**



The **My Partner** table provides an overview of all partners which have been created manually or imported from the Partner Registry (see below) and are therefore available for setting up an agreement.

[Info Icon] In case User Admin#Client Management is active only those local partners will be shown which are relevant for the active user.

The following functions are available to easily find the table entry you are looking for:

- All table heading have a **Sort** function (icon). Sort can be ascending and descending.
- Some table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.

8.1.1. Create a local partner

[Info Icon] A Local Partner could be for example a department within your organization.

Select **MESSENGER** on the navigation and you land on the **Partner** page. Click on the "*Create a new partner*" ⊕ icon, which opens the "*Create New Partner*" dialog box.

8.1.1.1. Enter New Backend ID

Enter a "**New Backend ID"** in the text box. The "*Local*" radio button for creating a Local Partner is selected by default. Then click on the "*Next Step*" button which brings you to the **Configuration** page for the new partner. The Backend ID and type of partner is displayed below the sub-navigation bar. The next step is to specify the configuration details for this new Local Partner. There are different accordion tabs › for the following configuration segments: **Identification**, **Communication**, **Schema Sets**, **Default Packager** and **Contact Information**.

You can only save a new Local Partner configuration when you have filled out all mandatory values marked with an asterisk (*). If you haven't filled out the mandatory fields when you click on the save 🖫 icon, an error message in red will be displayed underneath the field with the missing value. Please scroll down and make sure you have checked all fields in case you have received an error message.

8.1.1.2. Enter Identification settings

On the **Identification** segment, you can edit the different IDs used to refer to the given partner (in this case your new Local Partner):

Default IDs: By default, the Partner Display Name, the Backend Partner ID and the Party IDs are all set to the same value when a new Partner is created. In the Identification segment you can modify these settings if required.

- **Partner Display Name** – the Display Name is used within PONTON X/P in menus, selection lists, etc.
- **Backend Partner ID** – this identifier is used internally by PONTON X/P for communication with the backend and the file system. Hence this ID should match the ID in your respective backend system.
- **Party ID** – the Party ID is used for the identification of business partners in the messaging process. Please note that the Party ID at the senders end must match the Party ID at the receivers end. For each Partner, you can configure several party IDs. You can add additional Party IDs if required by clicking on the + icon. You must also select a Party-ID-Type for the new Party ID. It is possible to delete Party IDs by clicking on the delete 🗑 icon. Please note that at least one Party ID is required. When you send a message to a partner, all the party IDs you have defined for your own partner entry ('self') will be included in the Message. The receiver can then identify you as the sender if one of these party IDs matches a partner party ID in the receiver's partner configuration.

[Info Icon] **Party ID**

Party IDs are used to identify partners externally. To avoid name clashes and duplication, well-known naming Schemas exist to identify partners, e.g., DUNS codes, VAT numbers, IANA codes etc. For this reason, trading partners should agree on a minimal set of identification types (like DUNS numbers and IANA codes) that is to be used by all partners.

- **Party-ID-Types**: Select a Party-ID-Type from the list in the drop-down menu. Each party ID has a specific party ID type. Please note that you can configure only one party ID per type.
- **EbXml**: Enable EbXml20 if you want to use this party ID with EbXml20.
- **AS4:** Enable AS4 if you want to use this party ID with AS4.

8.1.1.3. Enter Communication settings

The communication settings specify the URIs of Partner's Messenger Service for the supported communication protocols. Enter the address to be used to access the partner's Messenger via the given protocol, for example: https://partner.server:8080/pontonxp/SoapListener. It is possible to use several URIs per protocol. This allows you for example to set up different Listeners for one partner by varying the address like http://partner.server:8080/pontonxp/AS2Listener. In case the partner can be reached at multiple URIs it is possible to define a fallback URI. If the Ping-All feature is activated, the Messenger switches to the defined fallback URI in the agreement if the partner is unreachable via the primary URI.

In the **Communication** tab, enter the communication settings for your new Partner configuration. Please specify the access details for the communication protocols you want to support: HTTP(S), SMTP, SMIME and FTP(S).

[Info Icon] **Limitation**

FTPS does not support TLSv1.3 connections.

- **URI of Messenger Service** – when defining the URI for HTTP(S) or FTP(S), please be sure to include the port. For example: http://your.server.com:8080/pontonxp/SoapListener
- **Preferred/Fallback**: By default the initial URI is marked as preferred. You can select additional URIs by clicking on the + plus icon and define which URI is the preferred URI or a fallback URI. It is only possible to select one preferred URI. It is possible to delete URIs by clicking on the delete icon.
- **Parallel Deliveries**: Defines the maximum number of parallel transfers started to the given URI

8.1.1.4. Activate Schema Sets

The Schema Sets section allows you to specify which schema sets are "allowed" for message exchanges with this Local Partner. The actual set of Schemas to be used can be specified individually in each **Partner Agreement**. In the Schema Sets table you will see a list of the Schema Sets installed on your Messenger system. Each entry in the list comprises the following elements:

- A checkbox for activating/deactivating the given Schema Set.
- The name of the Schema Set.

- An unfold/fold icon to hide/view the document types for each Schema Set
- A numerical entry indicating the number of selected/defined document types in the Schema Set – for example, 8/10 means that there are 10 document types included in the schema set and 8 of them are currently activated.

You can select all Schema Sets by selecting the checkbox ☐ in the Header row, or all document types of a particular Schema Set by selecting the checkbox ☐ next to the Schemaset. You can also select individuell document types contained in a Schema Set. Expand the Schema Set by clicking on the accordion tab › and select the document types by selecting the the checkbox ☐ . The number of selected document types and available document types in the Schema Set is highlighted in a yellow badge next to the name of the Schema Set.

8.1.1.5. Select Default Packager

You must select a default packager from the drop-down menu.

8.1.1.6. Enter Contact Information

We recommend to enter the contact details of your main contact person so that your business partner can contact if required.

- **Contact Name**
- **E-Mail**
- **Phone number**

8.1.2. Create a remote partner

> [Info Icon] A **remote** partner – refers to your business partners, for example: customers, suppliers, carriers, warehouse operators, etc.

Select **MESSENGER** on the navigation and you land on the **Partner** page. Click on the "*Create a new partner*" icon ⊕ which opens the "Create New Partner" dialog box. Click on the save 🖫 icon after you have filled out the required and optional fields below:

8.1.2.1. Enter New Backend ID

Enter a "**New Backend ID"** for your new remote partner in the text box and select the "*Remote*" radio button. Then click on the "*Next Step*" button, which opens the **Configuration** page for the new partner. The Backend ID and type of partner is displayed below the sub-navigation bar. The next step is to specify the configuration details for this new Remote Partner. There are different accordion tabs › for the following configuration segments: **Identification**, **Communication**, **Schema Sets**, **Default Packager** and **Contact Information**. You can only save a new Remote Partner configuration when you have filled out all mandatory values marked with an asterisk*. If you haven't filled out the mandatory fields when you click on the save 🖫 icon, you will receive an error message in red will be displayed underneath the field with the missing value. Please scroll down and make sure you have checked all fields in case you have received an error message.

8.1.2.2. Update partner automatically from the registry

If the **Automatic updates** option is activated, the profile for the Remote Partner will be downloaded from the registry automatically whenever it changes, while you can not change this Partner manually. This is only the case, however, if the global setting to **Enable automatic updates** has been activated in the profile registry configuration.

8.1.2.3. Update agreements automatically

If the **Automatic Agreement updates** option is activated all the existing agreements with this remote partner will automatically be recreated as soon as the profile of this remote partner has been downloaded from the registry.

8.1.2.4. Allow certificate update from received messages

If the **allow certificate update from received messages** option is activated, the certificates from incoming messages are not just accepted, but also installed on the remote partner profile while processing incoming messages with an unknown partner certificate.

[Info Icon] This automatic certificate update is only possible if the corresponding CA certificate is already known within the messenger, the certificate is not expired and a valid partyID match is found with the partner profile.

8.1.2.5. Enter Identification settings

On the **Identification** tab, you can edit the different IDs used to refer to the given partner (in this case your new Remote Partner):

Default IDs: By default, the Partner Display Name, the Backend Partner ID and the Party IDs are all set to the same value when a new partner is created. In the Identification tab you can modify these settings if required.

- **Partner Display Name** – the Display Name is used within PONTON X/P in menus, selection lists, etc.
- **Backend Partner ID** – the Backend Partner ID is used for communication with the backend (ERP) system.
- **Party ID** – the Party ID is used for the identification of business partners in the messaging process. Please note that the Party ID at the senders end must match the Party ID at the receivers end. For each Partner, you can configure several party IDs. You can add additional Party IDs if required by clicking on the + icon. You must also select a Party-ID-Type for the new Party ID. It is possible to delete Party IDs by clicking on the delete icon. Please note that at least one Party ID is required. When you send an XML message to a partner, all the party IDs you have defined for your own partner entry ('self') will be included in the Message. The receiver can then identify you as the sender if one of these party IDs matches a partner party ID in the receiver's partner configuration.

> ⚠ **Identical Party IDs**
>
> Please ensure that identical Party IDs are used in the sender's as well as receiver's messenger

configuration – otherwise there will be errors when you attempt to exchange messages with your partners. Other Party ID types can also be used, for example EIC, Duns Number, GLN (Global Location Number) or URI. For a single partner you can create multiple Party IDs by using different Party ID types.

- **Party-ID-Types**: Select a Party-ID-Type from the list in the drop-down menu. Each party ID has a specific party ID type. Please note that you can configure only one party ID per type.
- **EbXml**: Enable EbXml20 if you want to use this party ID with EbXml20.
- **AS4:** Enable AS4 if you want to use this party ID with AS4.

8.1.2.6. Enter Communication settings

The communication settings specify the URIs of Partner's Messenger Service for the supported communication protocols. Choose a protocol and enter the address to be used to access the partner's Messenger via the given protocol, for example: https://partner.server:8080/pontonxp/SoapListener. It is possible to use several URIs per protocol. This allows you for example to set up different Listeners for one partner by varying the address like https://partner.server:8080/pontonxp/AS2Listener. In case the partner can be reached at multiple URIs it is possible to define a fallback URI. If the Ping-All feature is activated, the messenger switches to the defined fallback URI in the agreement if the partner is unreachable via the primary URI.

In the **Communication** tab, enter the communication settings for your new Partner configuration. Please specify the access details for the communication protocols you want to support: HTTP(S), SMTP, SMIME and FTP(S).

- **URI of Messenger Service** – when defining the URI for HTTP(S) or FTP(S), please be sure to include the port. For example: http://your.server.com:8080/pontonxp/SoapListener
- **Preferred/Fallback**: By default the initial URI is marked as preferred. You can select additional URIs by clicking on the + plus icon and define which URI is the preferred URI or a fallback URI. It is only possible to select one preferred URI. It is possible to delete URIs by clicking on the delete icon.
- **Parallel Deliveries**: Defines the maximum number of parallel transfers started to the given URI

8.1.2.7. Activate Schema Sets

The Schema Sets section allows you to specify which schema sets are "allowed" for message exchanges with this Remote Partner. The actual set of Schemas to be used can be specified individually in each **Partner Agreement**. In the Schema Sets table you will see a list of the Schema Sets installed on your Messenger system. Each entry in the list comprises the following elements:

- A checkbox for activating/deactivating the given Schema Set.
- The name of the Schema Set.
- An unfold/fold icon to hide/view the Schema Set Type for each Schema Set
- A numerical entry indicating the number of selected/defined document types in the Schema Set – for example, 8/10 means that there are 10 document types included in the schema set and 8 of them are currently activated.

You can select all Schema Sets by selecting the checkbox ☐ in the Header row, or all document types of a particular Schema Set by selecting the checkbox ☐ next to the Schemaset. You can also select individuell document types contained in a Schema Set. Expand the Schema Set by clicking on the accordion tab › and select the document types by selecting the the checkbox ☐. The number of selected document types and available document types in the Schema Set is highlighted in a yellow badge next to the name of the Schema Set.

8.1.2.8. Select Default Packager

You must select a default packager from the drop-down menu. The packager specifies how the messages sent by this partner will be packaged for transmission and backend processing. You can choose between different packaging standards, that offer diverse options to specify whether the relevant packaging elements will be used by this partner. EbXML, AS2 and AS4 are most widely used. For details on the specific settings please refer to the descriptions of packaging elements in the **Agreements** section.

8.1.2.9. Enter Contact Information

We recommend to enter the contact details of your main contact person so that your business partner can contact if required.

- Contact Name
- E-Mail
- Phone number

8.1.2.10. Add Maintenance Period

You can add one or several maintenance periods by clicking on the + plus icon which opens the input field for "From" (start date/time of the maintenance period) and "To" (end date/time of the maintenance period). Clicking in the input field opens a date picker. Use the date picker to enter dates. The date picker is showing always the current date / time. Change the time first and then click on date you want to select. As soon as you click on the date the date picker will close and the selected date is displayed in the input field. Please ensure you have selected dates in the future and that the end date is after the start date. It is possible to delete a Maintenance Period by clicking on the delete 🗑 icon.

8.1.3. Delete partner(s)

Go to My Partners and select one or several partner by clicking on the checkbox on the left hand side in the table row. The number of selected partners is displayed next to the delete icon 🗑. Click on the delete icon 🗑 and confirm that you want to delete the partner. Alternatively you can delete a single partner which you have selected for editing by clicking on the delete icon 🗑.

8.1.4. Synchronize partner profile with the registry

Go to My Partners and select one or several partner with the checkbox on the left hand side in the table row. The number of selected partners is displayed next to the synchronise 🔄 icon. Click on the synchronize icon to start the synchronisation process. A synchronised partner will be marked

with a green check ✅ symbol.

Partner Profile Status:

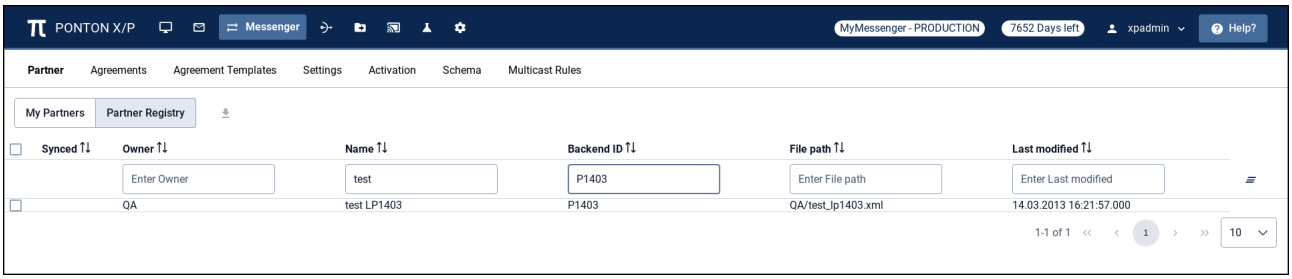
- **Valid**: if no installed certificate is expired (A valid partner is marked with a green check ✅ symbol)
- **Synced**: if the partner profile is available in the partner registry and has the same modification timestamp

⚠️ Please note that the Messenger has to establish a connection with the registry in order to compare the current partner configuration with the profile stored in the registry.

8.2. Partner Registry

Go to: **MESSENGER ⇄ > Partner > Partner Registry**

If you and your communication partners use the Partners Registry then exchanging Partner profiles is very simple. You find a list of all Partner when clicking on the "*Partner Registry*" tab in the **Messenger > Partner** section.



The following functions are available to easily find the table entry you are looking for:

- All table heading have a **Sort** function (icon). Sort can be ascending and descending.
- Some table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.

8.2.1. Import partner profiles

To import one or more available profiles select one or several partner with the checkbox on the left hand side in the table row. The number of selected partners is displayed next to the import ⬇ icon. Click on the import icon to start the import process which automatically imports all available profiles from the registry into your local messenger. Profiles which have been modified since the last import are missing the Synced symbol in the Partner Registry table. Go to My Partner and click on synchronise in order to automatically download the modified partner profiles into the messenger.

Synchronised partners will be marked with a green check symbol.

> ⚠ **Profile collision**
>
> Profiles which may collide with already existing profiles within your Messenger will not be imported.

8.3. Individual Partner configuration

8.3.1. Edit a Partner

Select a Partner (local or remote) by clicking on the edit icon which will appear on the right hand side of the table row when you hoover with your mouse over the Partner you want to edit. When you click on the edit icon the Partner configuration page opens. You can also right click the edit icon with the mouse and open the Partner configuration page in a new tab or new window. You can go back to the **My Partner** page by clicking on the **"Back to Partner"** button or leave the partner area by clicking on the navigation or sub-navigation bar. In case you have made changes to the partner, you will be asked to confirm that you want to leave the configuration page. You can change any of the fields on the configuration page, however you must enter valid values in the mandatory fields marked with an asterisk*. Click on the save icon after entering or editing the configuration.

8.3.1.1. Disable a partner

This option allows you to disable a specific partner within your Messenger configuration, without deleting the partner configuration. In this case the Messenger will reject any message received from this Partner. Select the "Partner disabled" checkbox and click on the save icon.

8.3.1.2. Re-enable a partner

Un-Select the "Partner disabled" checkbox and click on the save icon.

8.4. Certificates

> ⚠ PONTON X/P supports X.509 certificates in binary (DER) as well as text format (PEM).

8.4.1. Partner Certificates

In order to request, install, export, delete or make changes to the Partner Certificates settings you need select a specific Partner (local or remote) by clicking on the edit icon which will appear on the right hand side of the **My Partner** table row when you hoover with your mouse over the partner in the list. After clicking on the edit symbol the Partner configuration page opens. Click on the **Certificates** tab next to the Configuration tab to access the Certificates section.

8.4.1.1. Request a new partner certificate

> ⚠ **Remote partner certificates**
>
> In the case of **Remote Partners** you would receive the certificate from the partner directly or by downloading the partner's profile from the registry.

Requesting a Partner Certificate is only required for Local Partners. Click on the request new certificate icon + which opens the request certificate dialog box. Fill in the certificate request form for a single certificate. The mandatory fields are marked with an asterisk*:

- **Certificate Name; Organisation; E-mail address**
- **Country (select); Key pair (select)**
- **KeyPair** defines the algorithm, to generate the PrivateKeyPair.
- **Private key password**
- **Repeat password**

Optional input fields are: Department; Locality; State or province; Phone number; Fax number. You can also select to build the request with PONTON attributes. When you have filled out all required fields the "*Request certificate button*" becomes active. When you click on "*Request certificate button*" the requested certificate will appear in a new modal window which enables you to copy the certificates text to a clipboard or download the certificate as a .pem file. Close the window by clicking on the "*OK*" button. The requested Certificate will also appear in the Requested Certificates table. You can view the requested certificate by clicking on the view certificate icon in the Certificate Request column.

> ⚠ **Private password key**
> Please remember the private key password so that you can install the requested certificate later and prove that this certificate is actually yours.

8.4.1.2. Request a new certificate triple (TLS, SIGnature und ENCryption) for AS4-BDEW communication

Click on the request new SM-PKI certificate triple icon which opens the request certificate dialog box. Fill in the certificate triple request form to submit and receive a CRMF request that can be sent to your Sub-CA which will return 3 certificates (signatures, encryption and TLS).

The mandatory fields are marked with an asterisk *:

- **Org (CN)**
- **E-Mail address**
- **AS4-URL** only supports https urls. Wildcards are not allowed!
- **Country (select)**
- **Private key password**

- **Repeat password**

Optional input fields are: Market Partner-ID(=OU, Organisational Unit); Extension(=CN<extension>); Street; State; Postal code; City.

Hint: The messenger generates certificate triple requests with CN=<Organisation >.EMT[.<Extension>]. When you have filled out all required fields with valid inputs the "*Request certificate button*" becomes active. When you click on "*Request certificate button*" the requested certificate triple will appear in a new modal window which enables you to copy the certificate triple text to a clipboard or download the certificate triple as a .pem file. Close the window by clicking on the "*OK*" button. ⚠ The requested certificates (=three) will then appear in the Requested Certificates table individually. You can view the requested certificates by clicking on the view certificate icon in the Certificate Request column.

> ⚠ **Private password key**
>
> Please remember the private key password so that you can install the requested certificates later and prove that these certificates are actually yours.

8.4.1.3. Extending a partner certificate

You can also request a new certificates for an existing certificate that is going to expire in the near future. In that case click on the request certificate icon, which appears on the right hand side of the Partner certificate table row when you hoover with your mouse over the Partner certificate for which you want to request a new certificate. On click the "*Request certificate*" dialog box opens. The certificate request form is pre-filled with the details of the existing certificate, but can be changed. The mandatory fields are marked with an asterisk. when you have filled out all required fields the "*Request certificate button*" becomes active.

8.4.1.4. Install a partner certificate

When you have received a certificate file from a CA or a communication partner, open the "*Install Partner Certificate"* Dialog by clicking on the Install Certificate icon. Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid and you have entered the required password (local partner only) can click on the "*Install*" button to start the installation process. When the installation was successful the new certificate will disappear in the Partner certificates list.

> ⚠ **Local Partner certificate**
>
> For **Local Partner** you will need to enter the private key password (i.e. the password you entered when you filled in the certificate request for this particular certificate) to confirm that this certificate is actually yours.

> ⚠ **CA certificate**

A partner certificate will only be accepted when the certificate of the issuing CA (certificate authority) has been installed. Otherwise the trust relationship between the partner and the CA cannot be traced. The certificate for the PONTON CA is automatically included in the default installation. For other certificate authorities you will need to obtain and install the relevant CA certificate.

8.4.1.5. Export a partner certificate

[Info Icon] Exporting a certificate enables you to save and then reuse your own certificate as long as it is valid.

Click on the export icon, which appears on the right hand side of the Partner certificate table row when you hoover with your mouse over the Partner certificate you want to export. When you click on the export icon, the "*Export Certificate*" dialog will appear. Select either Base64 PEM or Binary DER as format for the exchange of your partner certificate with remote communication partners. If you want to use the Partner certificate for other Local Partners in the same or a different Messenger you need to export the certificate with a private key password. Select that option and enter the private key password. Clicking on the "*Export*" button will download the Partner Certificate to your local folder. You can share your certificate with your business partners by sending the certificate file to them via e-mail and having them install it into their partner configurations.

8.4.1.6. Delete a partner certificate

Click on the delete icon, which appears on the right hand side of the Partner certificate table row when you hoover with your mouse over the Partner certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the Partner certificate.

8.4.1.7. Define default Certificates

You can install multiple Certificates for Partners. This enables you to use different certificates for functions like signing and encryption or for different partners. It is also possible to define certificates for different packagers such as AS1, AS2, EbXml etc. In that case the Agreements subsequently created for this Partner will automatically use the packager certificates as defined in Partner certificates. Move the slider next to the listed packager (EbXml, AS4, AS3, AS2, AS1 or Processing) to the right so that the radio-button in the respective column become active. Click on the radio-button so that the circle is filled in blue and click on the save icon. You can also select which installed certificate you want to use as default certificate by clicking on the radio-button under the Default heading. Only one certificate can be used as default certificate.

⚠ Default Certificate

If 'default' certificate is chosen in the packager, the certificate used by the packager will automatically be updated as soon as another certificate is defined as the 'default' partner certificate.

Click on the save icon after you have made changes to the Partner certificate settings.

> ⚠ **Default certificate**
>
> All certificates that you install for one Partner will become default certificate in the order of their valid-from date. Alternatively, you can manually select the default certificate and the certificate that should be default when this certificate expires.

8.4.2. CA Certificates

In order to install, export or delete CA certificates you need select a specific Partner (local or remote) by clicking on the edit icon which will appear on the right hand side of the **My Partner** table row when you hoover with your mouse over the partner in the list. After clicking on the edit symbol the Partner configuration page opens. Click on the **Certificates** tab next to the Configuration tab to access the Certificates section.

8.4.2.1. Install a CA certificate

After requesting for a new certificate, you shall receive a valid certificate file via e-mail from the PONTON CA. Open the "*Install Partner CA Certificate*" dialog by clicking on the Install CA Certificate icon . Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. When the file is valid you can click on the "*Install*" button to start the installation process. If the installation was successful, the new CA Certificate will disappear in the CA Certificates list.

8.4.2.2. Export a CA certificate

Click on the export icon, which appears on the right hand side of the CA Certificate table row when you hoover with your mouse over the CA Certificate you want to export. When you click on the export icon, the "*Export CA certificate"* dialog will appear. Select either Base64 PEM or Binary DER as format. Clicking on the "*Export*" button will download the CA Certificate to your local folder.

8.4.2.3. Delete a CA certificate

Click on the delete icon which appears on the right hand side of the CA certificate table row when you hoover with your mouse over the CA Certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the CA Certificate.

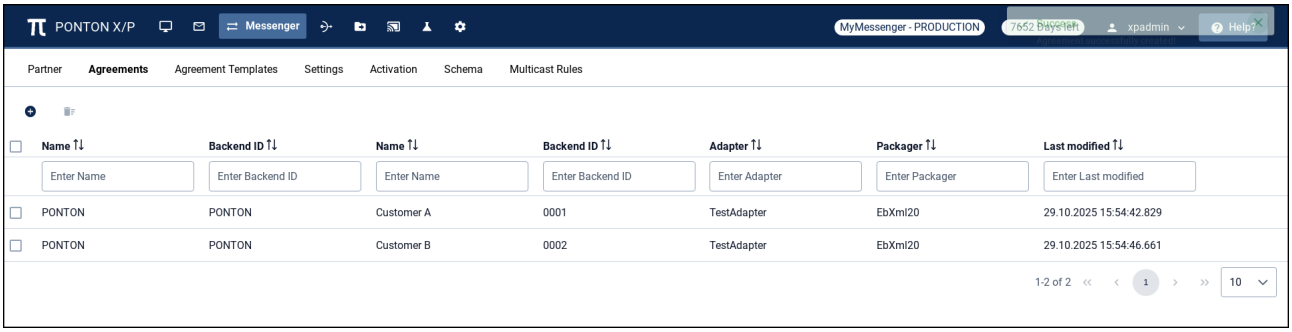
9. Messenger >Agreements

Go to: **MESSENGER** ⇄ > **Agreements**

The purpose of Partner Agreements is to specify the communication and data processing settings to be used when Messages are exchanged between two specific Partners. Each Agreement applies to a given combination of a Own and a Communication Partners.

9.1. View Agreements list

[Info Icon] In case User Admin#Client Management is active only those local partners and adapters will be provided which are relevant for the active user.



The **Agreements** table provides an overview of all Agreements which have been created in the Messenger. If the agreement is valid the symbol ✅ is shown. In case the agreement is not valid, the symbol ❌ is shown.

An agreement is invalid if:

- no message type is activated
- at least one activated message type is not accepted by sender or receiver
- no communication URL is defined for the receiver
- no party-id is defined for sender or receiver
- message signing is enabled but the sender has no valid certificate installed
- message encryption is enabled but the receiver has no valid certificate installed

The following functions are available to easily find the table entry you are looking for:

- All table headings have a **Sort** function (icon). Sort can be ascending and descending.
- Some table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.

9.2. Create a new Agreement

Go to **MESSENGER** ⇄ on the navigation and select **Agreements** in the sub-navigation bar. Click on the "Add Agreement" ⊕ icon, which opens the "*New Agreement*" dialog box. Select with the drop-down menu your Own Partner (Partner 1) and the intended Communication Partner (Partner 2) for the new Agreement. Then select an Agreement template from the drop-down menu. The Agreement templates differ with regards to the default options for **processing** and **packager settings**. You can not change the template for already created Agreements. If you want to change the template of an existing Agreement you need to delete the Agreement and create a new one.

Available default templates are:

- **EbXml20**
- **AS1**
- **AS2**
- **AS3**
- **AS4-ENTSOG**
- **Plain**

Then click on the "*Next Step*" button which opens the Agreement configuration page. The next step is to specify the configuration details for this new Agreement. There are different accordion tabs › for the following configuration segments: **Processing, Packager, Schema Set, Integration** and **Communication**. Click on the save 💾 icon after you have checked fields below.

[Info Icon] **Agreements between two local partners**

Before you can create an Agreement between two Own Partners "*Allow loopback*" in **Messenger → Settings → General Settings→ Communication** must be enabled.

⚠️ While preparing the messages for outbound communication the Agreement settings are applied sequentially in the following order - **Processing, Packaging and then Communication**. In case of incoming messages the agreement settings are applied in the order - **Packaging, Processing and then Integration**.

9.2.1. Enter Processing settings

The available processing settings for the **Agreement Template** (EbXml20, AS2, AS3, AS4-ENTSOG, Plain) are identical, with the exception that additional options are pre-selected for EbXmL. The processing settings are applied to the payload and allow to sign and/or encrypt the message content (payload).

[Info Icon] XML Modifications are optional settings if special treatment is required for xml files received from / delivered to the backend. XML Modification enables change in encoding

and the line ending of a document before sending or after receiving it, so that it is adapted to the requirements of the receiver or of an interior adapter. Additionally, there are options to change some XML elements in the payload that are especially helpful to guarantee the compatibility with older papiNet standards (version 1.0 and 1.1).

- **Modify sending XML payload**:
  - **Update papiNet 1.x Envelope for sending payload**: PapiNet 1.x documents have envelope information in the payload. If this option is enabled the protocol, the message ID, the time stamp, the sender and the receiver will be set to right values.
  - **Change Character Encoding:** The document can be converted to UTF-8 and UTF-16, several ISO encodings and some encodings for Japanese text.
  - **Change Line Ending**: The line endings in the document can be changed to the LF, CR or CR LF.
  - **Change DTD doctype**: A DTD (document typ definition) can be added or removed
  - **Pretty Print:** XML documents are reformatted to increase human readability. It has no effect on the XML structure itself, however it can help badly implemented xml parsers to process the document.
- **Modify received XML payload**:
  - **Update papiNet 1.x Envelope for received payload**: PapiNet 1.x documents have envelope information in the payload. If this option is enabled the protocol, the message ID, the time stamp, the sender and the receiver will be set to right values.
  - **Change Character Encoding:** The document can be converted to UTF-8 and UTF-16, several ISO encodings and some encodings for Japanese text.
  - **Change Line Ending:** The line endings in the document can be changed to the LF, CR or CR LF.
  - **Change DTD doctype**: A DTD (document typ definition) can be added or removed
  - **Pretty Print:** XML documents are reformatted to increase human readability. It has no effect on the XML structure itself, however it can help badly implemented xml parsers to process the document.
- **Sign payload:** If enabled the message will be signed. If activated you have to select the needed signature algorithm. You can select one specific certificate for signing in case you have installed multiple certificates for your Own Partner and want to use a non default certificate.
- **Include signing cert:** If enabled the used certificate is sent with the message.
- **Process signed payload:** Enable if you expect signed payloads.
- **Compress payload:** Specifies whether compression is to be used.
- **Process compressed payload:** Enable if you expect compressed payloads.
- **Encrypt payload:** If enabled the message will be encrypted. You can select one specific certificate for encryption in case you want to use a non default certificate of your Communication Partner.
- **Process encrypted payload:** Enable if you expect encrypted payloads.

- **Validate sending payload:** Enables XML validation for outgoing messages.
- **Validate received payload**: Enables XML validation for incoming messages.
- **Create Energylink XML format:** This creates an XML signature and applies XML encryption as specified by the Austrian Energylink. Only "EDA Wechselprozess" messages are affected.
- **Process Energylink XML format:** This validates XML signatures and decrypts XML encrypted content as specified by the Austrian Energylink. Only "EDA Wechselprozess" messages are affected.
- **Custom validation of sending payload:** Enables an extra payload validation step when sending payloads. A validation plugin has to be provided for this.
- **Custom validation of received payload:** Enables an extra payload validation step when receiving payloads. A validation plugin has to be provided for this.

9.2.2. Enter Packager settings

The packager settings define the messaging standard to be applied. It allows you to apply globally defined standards to communicate with external parties. The PONTON X/P Messenger supports ebXML 2.0, AS1, AS2, AS3 and AS4. Furthermore the Messenger also allows exchange of plain messages. The available packaging settings depend on the **Agreement Template** you have selected.

9.2.2.1. EbXML settings (EbXML template)

The following options are available to make messaging more compatible between individual parties, since different parties might only accept / send Messages which fulfill certain criteria. Mandatory fields are marked with an asterisk (*).

- **Role (from) / (to):** EbXML allows you to define a role for sender and receiver (e.g. 'buyer' and 'seller'). This has no effect for PONTON X/P, but other messaging software might require specific values.
- **Service**/Service Type:* The EbXML Service / EbXML ServiceType settings can be used to specify the EbXML service that handles the Message.
- **Action**:* This setting identifies a process within the specified EbXML Service.
- **CPA ID**:* The CPA ID specifies the parameters governing the exchange of messages between the parties.
- **Request Acknowledgements/Request signed acknowledgements:** Enable this option if you expect (signed) acknowledgements for sent messages.
- **Request Duplicate elimination:** If duplicate elimination is enabled, the receiver must eliminate duplicate messages.
- **Request synchronous reply** – If you use a synchronous protocol, a reply can be received through the same connection.
- **Attachment role** – EbXML allows you to define roles for the different attachment types. PONTON X/P uses these roles to identify attachments in case of multiple attachments.

⚠️ The following variables can be used in the options **Role To , Role From, Service, Service**

Type, Action, CPA ID: %MESSAGETYPE%, %TESTFLAG%, %MESSAGEVERSION%, %SCHEMASET%, %SENDERID%, %SENDER_DISPLAYNAME%, %RECEIVERID%, %RECEIVER_DISPLAYNAME%, %MESSAGEID%, %CONVERSATIONID%

9.2.2.2. AS1 settings (AS1 template)

AS1 is available for SMTP communication and the following settings are available for this standard:

- **Request acknowledgements:** You can request an MDN (Message Disposition Notification) for all outbound messages from your communication partner.
- **Request signed acknowledgements:** If you want the MDN to be signed, you have to activate this option. The MIC hash algorithm has to be selected from the list.
- **Expect Signed Acknowledgements:** Enable this option if you expect signed acknowledgements.
- **Sign messages:** If enabled the messages will be signed.
- **Expect signed messages:** Enable if you expect signed payloads.
- **Sign acknowledgements:** If enabled the acknowledgements will be signed.
- **Compress messages:** Specifies whether compression is to be used.
- **Expect compressed messages:** Enable if you expect compressed messages.
- **Encrypt messages:** If enabled the messages will be encrypted.
- **Expect encrypted messages:** Enable if you expect encrypted messages.
- **Mail subject:** This field defines the subject for all outgoing mails.
- **Use mail-client email format when sending mail with body content:** The Messenger creates a body part with a static text for all outgoing messages.
- **Accept mail-client email format:** If this option is activated the Messenger tries to process eMails that are not AS1-compliant (for example eMails created by eMail clients like MS Outlook).
- **Ignore duplicate messages**: If ignore duplicate elimination is set, the Messenger will ignore messages with previously received message-IDs.

9.2.2.3. AS2 settings (AS2 template)

AS2 is available for communication by HTTP(S) and the following settings are available for this standard:

- **Request acknowledgements:** You can request an MDN (Message Disposition Notification) for all outbound messages from your communication partner.
- **Request signed acknowledgements:** If you want the MDN to be signed, you have to activate this option. The MIC hash algorithm has to be selected from the list.
- **Asynchronous response URL:** If this option is enabled, then the receiver will send the requested MDNs to the specified URL.
- **Expect Signed Acknowledgements:** Enable this option if you expect signed acknowledgements.
- **Sign messages:** If enabled the messages will be signed.

- **Expect signed messages:** Enable if you expect signed payloads.
- **Sign acknowledgements:** If enabled the acknowledgements will be signed.
- **Compress messages**: Specifies whether compression is to be used.
- **Expect compressed messages:** Enable if you expect compressed messages.
- **Encrypt messages:** If enabled the messages will be encrypted.
- **Ignore duplicate messages**: If ignore duplicate elimination is set, the Messenger will ignore messages with previously received message-IDs.

9.2.2.4. AS3 settings (AS3 template)

AS3 is available for communication by FTP(S) and the following settings are available for this standard:

- **Request acknowledgements:** You can request an MDN (Message Disposition Notification) for all outbound Messages from your communication Partner.
- **Request signed acknowledgements**: If you want the MDN to be signed, you can select the algorithm.
- **Asynchronous response URL:** If this option is enabled, then the receiver will send the requested MDNs to the specified URL.
- **Expect Signed Acknowledgements:** Enable this option if you expect signed acknowledgements.
- **Sign messages:** You can select the algorithm with the drop-down menu to sign the Message with your Partner certificate. You can select one specific certificate for signing in case you have installed multiple certificates for your Local Partner.
- **Expect signed messages:** Enable if you expect signed payloads.
- **Sign acknowledgements:** If enabled the acknowledgements will be signed.
- **Compress messages**: Specifies whether compression is to be used.
- **Expect compressed messages:** Enable if you expect compressed messages.
- **Encrypt messages:** If enabled the messages will be encrypted.
- **Ignore duplicate messages**: If ignore duplicate elimination is set, the Messenger will ignore messages with previously received message-IDs.

9.2.2.5. AS4 settings (AS4-ENTSOG template)

Following settings are possible and can be defined while using the AS4 standard in the messenger, mandatory fields are marked with an asterisk*.

- **Role (from) / (to):** Role identifies the authorized role of the Party sending or receiving the message.
- **Service**:* This element identifies the service that acts on the message
- **Service type:** This indicates how the parties sending and receiving the message will interpret the value of the service element. If the type attribute is not set, the content of the Service element MUST be a URI.

- **Action**:* This string identifies an operation or an activity within the defined Service
- **Agreement reference:** The value of an Agreement reference element identifies the agreement that governs the exchange and must be unique within a namespace mutually agreed by the two parties.
- **Agreement reference type:** This attribute indicates how the parties sending and receiving the Message will interpret the value of the reference. If the type attribute is not present, the content of the AgreementRef element MUST be a URI
- **Agreement reference pmode**: This attribute indicates how the messaged is processed.
- **Send message properties:** If this is enabled, then message related information is added to the AS4 envelope as Type/Value pairs. These values include ProductName, VendorName as well as Version of the messaging tool. You can add individual properties. The value can be fixed or use a variable described below.
- **Send content properties:** If this is enabled, then payload related information is added to the AS4 envelope as Type/Value pairs. You can add individual properties. The value can be fixed or use a variable described below.
- **Support certificate update message:** If a new certificate is installed in a Local Partner profile, all Agreements for this profile will be checked. If the flag is enabled, a certificate update message will be sent. You need at least one certificate for the Local Partner installed. This is the implementation of the ENTSOG AS4 Profile ebCore Agreement Update feature, which follows the guidelines of the ebCore Agreement Update Specification.
- **Sign messages:** You can select the algorithm to sign the Message with your own certificate. In the outbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your Local Partner.
- **Expect signed messages:** Enable if you expect signed payload.
- **Compress messages:** You can select to compress the Message before sending.
- **Expect compressed messages:** Enable if you expect compression.
- **Encrypt messages**: You can select the algorithm to encrypt the Message with your Partner's Certificate.
- **Send receipts:** Enable this to send an AS4 receipt message for any received message.
- **Send signed receipts:** Sign AS4 receipt messages before sending.
- **Ignore duplicate messages:** If ignore duplicate elimination is set, the Messenger will ignore all received duplicate Messages
- **Send empty conversation ID**: Disables sending of conversation ID.

⚠️ The following variables can be used in the options **Role To , Role From, Service, Service Type, Action, AgreementRef**, **AgreementRefType, Message Property Value** and **Content Property Value**: %MESSAGETYPE%, %TESTFLAG%, %MESSAGEVERSION%, %SCHEMASET%, %SENDERID%, %SENDER_DISPLAYNAME%, %RECEIVERID%, %RECEIVER_DISPLAYNAME%, %MESSAGEID%, %CONVERSATIONID%

Since version 4.4.0 it is possible to use elliptic curve security for encryption of symmetric key and for signature. Therefore four ECDH-ES-ConcatKDF options were added to encryption

algorithm selectbox. They differs in the way of filling the ConcatKDF-parameters (empty ⇒ stay empty / generated ⇒ filled with random values) and the hash algorithm to use (SHA256 / SHA512). To sign with elliptic curves you have to select ECDSA as signature algorithm.
Both requires, that the private key pair was generated with corresponding type, f.e. **brainpoolP256r1.**

9.2.2.6. Plain settings (Plain template)

Is available for HTTP(S) and FTP(S). Plain packaging allows sending and receiving pure messages without any packaging envelope. This packaging option is intended for the communication with a Partner that does not have a messaging software.

- **Use transport results as acknowledgement:** If enabled transport level results will be converted to Acknowledgement and sent to the specified Adapter.
- **Reception password:** The optional password is used to secure the reception of messages. If no password is defined, any Message that is posted to the PlainListener URL will be accepted.

9.2.3. Configure Schema Set

The Schema Sets section allows you to specify which Schema Sets are to be used for message exchange based on the current Partner Agreement. To access the **Schema Sets go to MESSENER** > **Schema Sets** sub-navigation tab.

⚠ Schema Sets

The Schema Sets available for selection in a given Partner Agreement are dependent on the schema settings in your partner profiles for the two relevant partners. Please keep in mind, however, that this consistency check is local, i.e. it applies to the partner profiles and Agreements in your own Messenger configuration. To ensure successful message exchange with your communication partners you will need to cross check the selected options (as well as your other configuration settings) with your Partners.

9.2.4. Enter Integration details

9.2.4.1. Select Default Adapter

Default Adapter:* the selected adapter will be used for all received messages unless overridden by an adapter rule.

9.2.4.2. Define adapter rules

Click on the "*Define adapter rules*" button and enter the values for:

- **XPath***: Define a XPATH whose value will be compared with the VALUE by OPERATOR. If comparison matches, the adapter that will process the message will be changed. Special XPATH-expressions are available: '!MessageId', '!ConversationId', '!MessageType', '!MessageVersion', '!SchemaSet', '!TestFlag', '!LogInfo', '!Action', '!Service', '!OriginalFileName' and

'!ProcessedFileName'.

- **Operator***: Select of the following operator from the drop-down menu: EQUAL, NOT_EQUAL, LESS_THAN, GREATER_THAN, CONTAINS, CONTAINS_NOT, STARTS_WITH, ENDS_WITH
- **Value**:* Enter the value for the XPATH.
- **Adapter**:* Enter the Adapter that will process the message when the above condition is meet.

You can add additional **Adapter Rules** by clicking on the + icon. It is possible to delete Adapter Rules by clicking on the delete 🗑 icon.

⚠️ If multiple rules which might overlap are defined within the same agreement then only the last rule shall be effectively applied.

9.2.5. Enter Communication details

The communication settings define the communication URI for message delivery.

- **Reception URI**: This value cannot be changed. It displays the URI that a communication partner needs to send messages to this Messenger instance. The hostname and port depend on the network setup and cannot be detected automatically.
- ⚠️ While creating agreements the messenger pre-selects values for primary and fallback URLs based on the URLs provided in the remote partner profile (see Messenger >Partner#Enter Communication settings). It is recommended not to modify these URLs in the agreement if 'Ping All' is enabled.
  - **Primary URI***: Primary URI specifies the transport protocol to be used for sending messages based on this agreement. It is mandatory to set one URI.
  - **Fallback URI:** In case the partner is reachable at more than one URI, a fallback URI can be defined. The Messenger will use the fallback URI only if the primary URI has been identified as unreachable during previous transmission tries. The fallback channel is only used if the "PingAll" option is enabled in the agreement as well as globally under Messenger → Settings → General Settings→ Communication.
  - **PingAll enabled:** By activating this option, the Messenger will periodically verify that the defined communication URIs are usable.
- **Username/password:** Username / Password only needs to be provided if the URI can only be accessed after authentication.
- **Retries**:* Retries determines how often the Messenger will try to send a message until it receives an acknowledgement. It is mandatory to choose a retry value.
- **Retry Interval** (seconds)**:** Retry Interval determines how long the Messenger will try to send a message until it receives an acknowledgement. If less retry intervals than number of Retries are entered, then the last retry interval will be used for the remaining retries. You can add additional Retry Intervals by clicking on the + icon. It is possible to delete Retry Intervals by clicking on the delete 🗑 icon.

9.2.5.1. Define communication rules

With communication rules it is possible to override the regular transmission URI based on message

specific rules.

Click on the "*Define communication rules*" button and enter the values for:

- **XPath***: Define a XPATH whose value will be compared with the VALUE by OPERATOR. If comparison matches, the adapter that will process the message will be changed. Special XPATH-expressions are available: '!MessageId', '!ConversationId', '!MessageType', '!MessageVersion', '!SchemaSet', '!TestFlag', '!LogInfo'', '!Action', '!Service', '!OriginalFileName' and '!ProcessedFileName'.
- **Operator***: Select of the following operator from the drop-down menu: EQUAL, NOT_EQUAL, LESS_THAN, GREATER_THAN, CONTAINS, CONTAINS_NOT, STARTS_WITH, ENDS_WITH
- **Value**:* Enter the value for the XPATH.
- **URI**:* Communication URI that will be used when the rule is triggered

You can add additional **Communication Rules** by clicking on the + icon. It is possible to delete Communication Rules by clicking on the delete icon.

⚠ If multiple rules which might overlap are defined within the same agreement then only the last rule shall be effectively applied.

9.3. Edit an agreement

Go to **MESSENGER** > **Agreements** and select an agreement by clicking on the edit icon, which will appear on the right hand side of the table row when you hoover with your mouse over the Agreement you want to edit. When you click on the edit icon the **Agreement Configuration** page opens. You can also right click the edit icon with the mouse and open the Agreement configuration page in a new tab or window. You can go back to the **Agreement** page by clicking on the **"Back to Agreements"** button or leave the agreement area by clicking on the navigation or sub-navigation bar. In case you have made changes to the agreement, you will be asked to confirm that you want to leave the configuration page. You can change any of the fields on the configuration page, however you must enter valid values in the mandatory fields. Click on the save icon after entering or editing the configuration.

9.4. Delete agreements

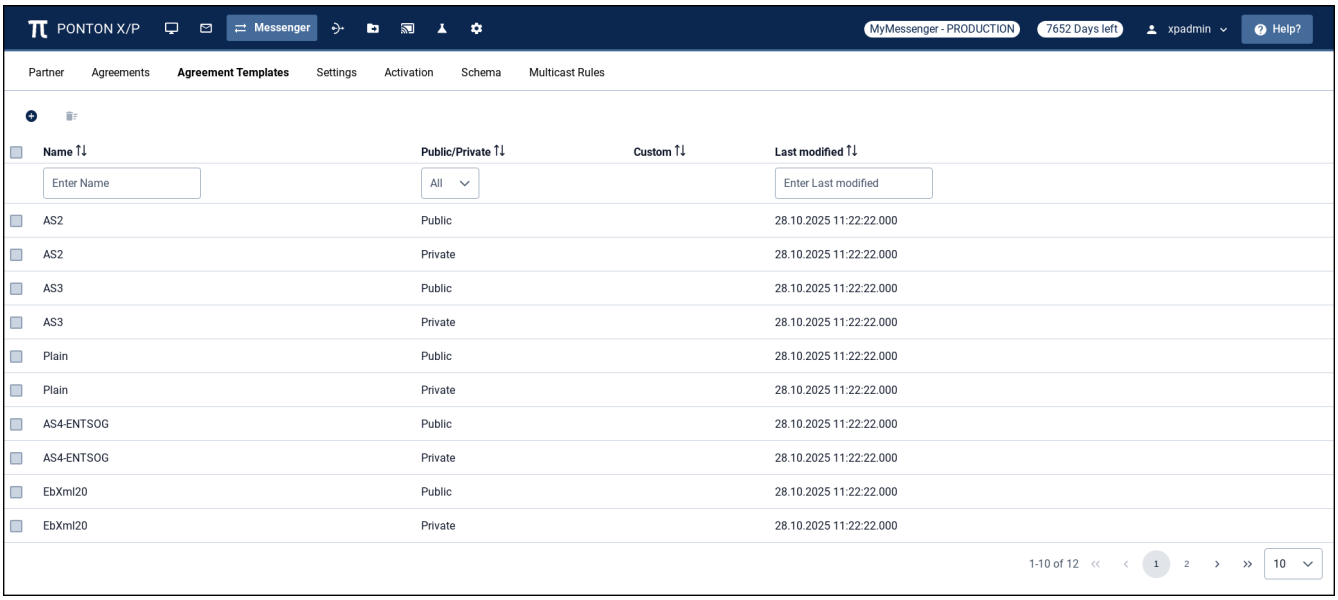
Go to **MESSENGER** > **Agreements** and select one or several Agreements by clicking on the checkbox on the left hand side in the table row. The number of selected Agreements is displayed next to the delete icon. Click on the delete icon and confirm that you want to delete the Agreement. Alternatively you can delete a single Agreement which you have selected for editing by clicking on the delete icon.

10. Messenger >Agreement Templates

Go to: **MESSENGER** ⇄> **Agreement Templates**

The purpose of Partner Agreement Templates is to define the communication and data processing settings for the Agreements. The Agreement Templates differ with regards to the default options for **processing** and **packager settings.**

10.1. View Agreement Template list



The Agreement Templates table provides an overview of all Agreement Templates which are available in the Messenger. An Agreement Template contains of two separate files, a public and a private file. It is necessary to have both files to use an Agreement Template properly. If an Agreement Template was created by the user it marked as custom with the symbol ✅. The other templates are default and will be provided in the Messenger.

Default templates are:

- **EbXml20**
- **AS1**
- **AS2**
- **AS3**
- **AS4-ENTSOG**
- **Plain**

The following functions are available to easily find the table entry you are looking for:

- All table headings have a **Sort** function (icon). Sort can be ascending and descending.
- Some table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.

- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.

10.2. Create a new agreement template

Go to **MESSENGER** ⇄ on the navigation and select **Agreement Templates** in the sub-navigation bar. Click on the "Add Agreement Template" ⊕ icon, which opens the "*New Agreement Template*" dialog box. Either choose a file one at a time by clicking on "*Choose files*" or drag-and-drop the two files into the marked area. The names will appear in the dialog box. You can remove the files by clicking on the ⊕ symbol. If the files are valid you can click on the "*Upload*" button to start the upload process. When the upload was successful the new template with two entries (one for private and one for public) will appear in the Agreement Templates list.

[Info Icon] **Private and public file**
It is required to upload two files at a time with a specific name pattern to create a valid Agreement Template. The names of the files should be agreementId_private.vm (e.g. EDA_private.vm) and agreementId_public.vm (e.g. EDA_public.vm).

10.3. Edit an agreement template

Go to **MESSENGER** ⇄ > **Agreement Templates** and select an agreement template by clicking on the edit ✎ icon, which will appear on the right hand side of the table row when you hover with your mouse over the agreement template you want to edit. When you click on the edit ✎ icon the "*Edit Agreement Template*" dialog box opens. Click on the "*Save Template*" button after editing the content of the agreement template file. It is possible to edit custom and default templates. If you edit a default template it will be marked as custom after the changes were saved.

[Info Icon] **Note**: These templates are **Apache Velocity templates**. The following variables are dynamically replaced during agreement creation.

10.3.1. Variables for Agreement templates

Table 1. Agreement object

Property	type	Description
agreement.adapterId	String	Default adapter ID
agreement.documentTypes	List<DocumentType>	List of automatically selected message types (DocumentType objects)
agreement.retries	Integer	Maximum number of default attempts
agreement.retryIntervals	List<Integer>	List of default retry intervals
agreement.ownPartner	Partner	Own partner

Property	type	Description
agreement.communicationPartner	Partner	Communication partner

Table 2. DocumentType object

Property	Type	Description
version	String	Message version
type	String	Message type
namespace	String	XML namespace
schemalocation	String	Schema location
schemaSet	String	Schema set name
rootElement	String	Root element

Table 3. Partner object

Property	Type	Description
id	String	Unique technical partner ID
displayName	String	Display name
backendPartnerId	String	Backend partner ID
primaryUrl	URL	Primary URL
fallbackUrl	URL	Fallback URL
partyIds	Map<String, String>	Map of partner identification tuples: key = PartyId type value = PartyId ID

Table 4. URL object

Property	Type	Description
id	String	Unique URL ID within partner configuration
url	String	Communication URL

10.3.1.1. Example template

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PrivateCollaborationAgreement>
    <DefaultAdapterId>${agreement.adapterId}</DefaultAdapterId>
    <Rules SenderRefId="${agreement.ownPartner.id}"
ReceiverRefId="${agreement.communicationPartner.id}">
    </Rules>
    <Rules SenderRefId="${agreement.communicationPartner.id}"
ReceiverRefId="${agreement.ownPartner.id}">
```

```
        <Rule id="1">
            <Trigger XPath="!MessageType" Operator="Equal" Value="MSCONS"/>
            <Action type="ChangeDestinationAdapter">MSCONS-Adapter</Action>
        </Rule>
    </Rules>
</PrivateCollaborationAgreement>
```

10.4. Download an agreement template

Go to **MESSENGER** ⇄ > **Agreement Templates** and select an agreement template by clicking on the download ⬇ icon, which will appear on the right hand side of the table row when you hover with your mouse over the agreement template you want to download. Clicking on the icon will download the agreement template file to your local folder.

10.5. Delete agreement templates

Go to **MESSENGER** ⇄ > **Agreement Templates** and select one or several custom Agreement Templates by clicking on the checkbox on the left hand side in the table row. The number of selected Agreement Templates is displayed next to the delete 🗑 icon. Click on the delete 🗑 icon and confirm that you want to delete the Agreement Template(s). If you delete a custom template which was created from a default template (by editing a default template) the default template will be restored automatically. PLease not that it is not possible to delete default templates.

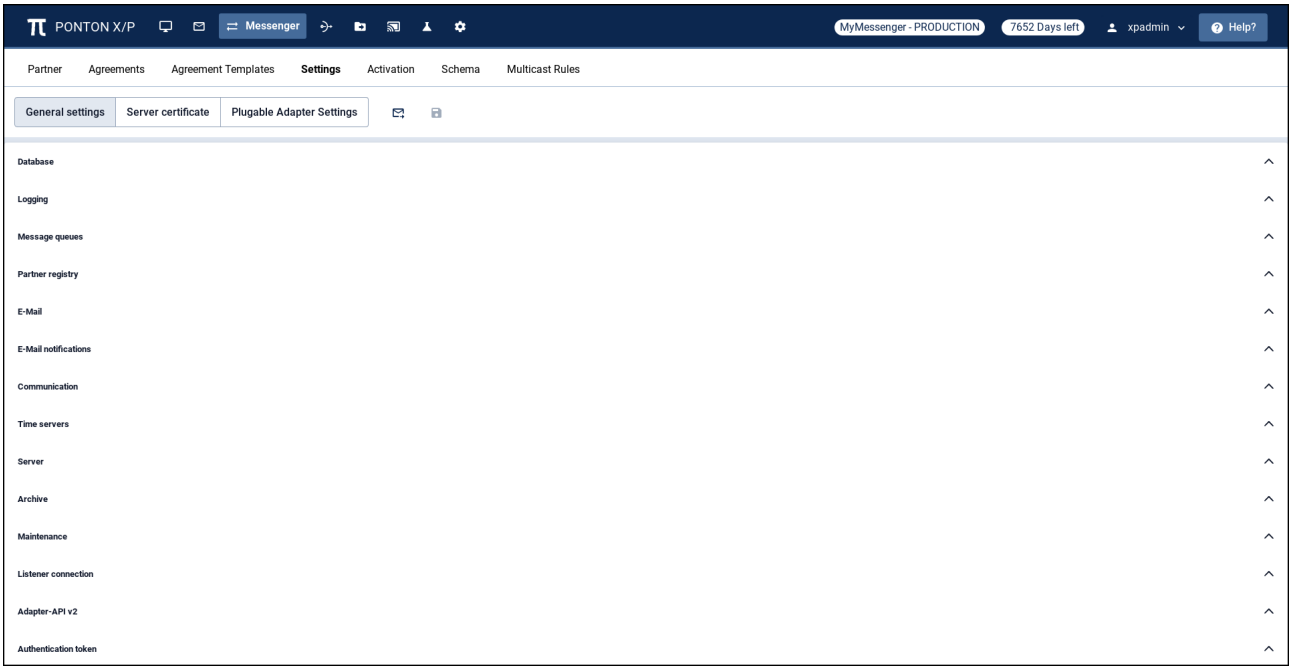
10.6. Customize agreement templates

There are two options for customizing agreement templates:

1. modify the default templates directly (see "Edit an agreement template")
2. create a new template by downloading an existing template (see "Download an agreement template")
   modify the copy with a text editor (see "Edit an agreement template" for format and variable details)
   rename and upload the new template. (see "Create a new agreement template")

11. Messenger >Settings

Go to: **MESSENGER** ⇄ > **Settings**



11.1. Test sending e-mail

Click on the **Test sending e-mail** ✉ icon to test the e-mail configuration. Enter a receiver e-mail address in the e-mail field and click on the "Send" button. If you want to close the dialog and not send the test e-mail, click on the **x** button.

11.2. General Settings

Click on the save icon 💾 after entering or editing values in any of the sections below.

11.2.1. Enter database settings

The Messenger stores log entries in a database. These information is related to the processing of messages through the Messenger. Content of the files transacted via the Messenger is not stored in the database tables used by the Messenger.

> [Info Icon] **HSQL database**
> PONTON X/P is installed with a pre-configured HSQL database, which is only intended for **test** purposes during the TRIAL period. For productive operations a supported database system must be used.

The database is accessed via JDBC connection. Setup of database is done automatically by PONTON X/P Messenger (for details see "Database Connection")
Database-Cleanup: Configure the Cleanup-Job, which deletes old messages from database.

- **Delete database entries:** Enables cleanup of database. [Info Icon] This is activated as per default settings.
- **Cleanup Time:** The time, when the Cleanup-Job should start. Default value is 03:00:00
- **Maximum runtime of Cleanup-Job:** The Cleanup-Job will stop when this maximum runtime is reached. The value 0 means, the Cleanup-Job will not stop before all old messages are deleted.
- **Maximum age:** Messages older than this age (in days) will be selected for deletion.

11.2.2. Define logging level

To specify the logging level please select the following settings, mandatory fields are marked with an asterisk*:

- **Messenger Log Level**: Select the desired level for Messenger logs. possible settings:
  - OFF - turns logging off completely
  - ERROR - only system errors, or processing errors are logged. The context of these errors is not visible.
  - INFO - only very few lines for each transmitted message are logged
  - DEBUG - many details of message processing steps are logged
  - TRACE - extensive logs are written. This should only be enabled for short periods to debug specific problems.
- **JDBC Log Level**: Select the desired level for database logs. possible settings:
  - OFF - turns logging off completely
  - DEBUG - logs SQL queries without values
  - TRACE - logs SQL values sent to the database (this results in very large log files and should not be enabled for long time).
- **Log only Errors in Database**: Logging all the message related events in the database reduces the performance but offers a better audit trail. This option allows to decide between maximum performance and maximum audit level.
- **OK Event Age (days)***: The number of days after ok events will be deleted automatically.

⚠️ Please keep in mind that the chosen logging level can have an effect on the performance of your system. In particular, it is advisable to use DEBUG or TRACE logging only while trying to troubleshoot and analyze errors.

11.2.3. Enter message queue settings

Mandatory fields are marked with an asterisk*:

- **Inbound Queue Scan Interval (milliseconds)***: specifies the interval to scan the inbound message queues.
- **Inbound Queue Delivery Timeout (seconds)***: specifies the maximum time-frame expected

for a successful message delivery to an adapter. The time-frame starts when a message is scheduled for delivery and ends when the Adapter acknowledges the correct reception. Whenever this expected time-frame is exceeded a warning message will be logged. In combination with the email notification this can be used to alert an administrator about the issue between Messenger and Adapter.
So if the delivery timeout is specified as 5 minutes, a warning will be created once after 5 minutes.

- **Inbound Queue Retry Delay (seconds)***: specifies the delay after an unsuccessful message delivery attempt. This is used to reduce load on the receiving Adapter.
- **Inbound Queue Notification Retry***: specifies how many times the failing of the delivery of a message to the adapter should be reported.
- **Outbound Queue Scan Interval (seconds)***: specifies the interval to scan the outbound message queue.

11.2.4. Enter Partner Registry Settings

The partner registry allows you to exchange profiles with other partners by uploading and downloading Partner configurations to/from a central registry. Here you can configure the connection and authentication to access the Partner Registry:

- **Registry URL:** enter the address where the Partner Registry is to be accessed. Leave it empty to use the default registry server.
- **Username** / Password**: enter the user name and password for access to the registry. These will be provided by the Partner Registry administrator.
- **Automatic agreement updates**: this option allows your Messenger to automatically update the already existing Agreements with a specific remote Partner as soon as the profile of this Remote Partner has been updated in the Messenger from the Partner Registry.
- **Automatic partner creation:** this option allows your Messenger to automatically download profiles when needed. The Messenger will try to find a Partner profile in the Partner Registry based on the **Backend Partner ID** for outbound Messages and based on the default **Party-ID** for inbound Messages. When this option is enabled, also Partner Agreements are created when needed.

⚠️ Currently the automatic partner creation option only works as intended when the Messenger is used in the Austrian EDA environment.

- **Automatic partner cleanup:** this option allows your Messenger to automatically delete remote profiles, which were deleted on the Partner Registry.
- **Download interval (hours)***: Defines the interval how often profile updates are downloaded from the registry.

[Info Icon] When updating the Partner Certificates from the Partner Registry the client certificates on the Listener are also updated automatically.

11.3. Enable E-mail

In this section you can enable or disable inbound and outbound e-mail connections in your Messenger configuration. Mandatory fields are marked with an asterisk*:

Inbound
You can enable your Messenger to receive e-mail messages by setting up a POP/IMAP connection with the following entries:

- **Protocol***: set to POP3 / IMAP (depending on the type of mail server)
- **Server***: the hostname or IP address of your mail server
- **Interval (seconds)***: the frequency for accessing the server for mail download
- **Username / Password***: must be properly set to authenticate the Messenger on the mail server
- **Inbox Folder***: the folder on the server where new emails are stored. use "INBOX" to access the default folder.

Outbound
This connection is used for e-mail messages sent by your Messenger to your business partners and also for notification emails to administrators. The following data can be configured if enabled, mandatory fields are marked with an asterisk*:

- **From***: the sender's address to be used for e-mails sent from the Messenger.
- **Protocol***: select the protocol from the available protocols in the drop-down menu.
- **SMTP**: the outgoing mail server to be contacted by your Messenger in order to submit the e-mail.
- **Username / password**: must be entered if your mail server requires authentication for outgoing e-mails, in this case enter the settings to be used by the Messenger to log in on the mail server.

⚠ Email configuration is required before being able to use AS1 packaging successfully.

11.3.1. Enter E-mail Notification settings

⚠ **E-mail notifications**
E-mail notifications require an outbound e-mail connection.

You can use the notification service to send e-mails to specified addresses whenever certain events occur. For example, you might want to notify your system administrator whenever certain errors are encountered. The Messenger distinguishes between message related notifications and application (or system) related events.

Add message events receiver
To receive a notification in case a message could not be processed as expected the user can choose

from a list of events for which he/ she requires a notification. This can be done by adding Message Event Receivers. Click on the "Add Message Event Receiver" button and enter the following, mandatory fields are marked with an asterisk*:

- **e-mail address***: Enter e-mail address of the e-mail recipient.
- **With HTML attachment**: Select the checkbox if you want to include the message content as HTML rendered attachment
- **Message event***: Select one or multiple message events from the drop-down list which will trigger an e-mail notification
- **Subject Elements***: The default subject of the e-mail notification will be as follows: "Notification for message" + Message ID You can customize the subject of the e-mail notification by selecting Subject Elements from the drop-down list. If you define several subject elements, they will be separated by blanks in the subject line. You can use the following element types:
  - **Text**: a static text that you enter in the text box.
  - **Variable**: a predefined variable such as the Message ID, the Message Type or the Receiver ID/Display Name.
  - **Xpath**: the xpath to an XML element/attribute contained in the payload message.

Please note that only a subset of the complete xpath syntax is supported for the definition of subject elements. In particular, the following restrictions apply:

- The xpath must be an absolute path starting with the root node of the payload document.
- The xpath must refer to an actual node within the document. In the case of multiple nodes that satisfy the xpath, the first occurrence will be used.
- Reference to node attributes is not possible.
- Use of conditional expressions is not possible.

> [Info Icon] The use of xpath values as notification subject elements may lead to decreased performance, because the entire payload message has to be parsed in order to resolve the xpath expression.

You can add additional Subject Elements by clicking on the + icon. It is possible to delete Subject Elements by clicking on the delete icon.

Add system events receiver
To receive a notification in case the application is experiencing an unexpected situation the user can choose from a list of events for which he/ she requires a notification. To specify an address and event(s) click on the "Add System Event Receiver" button. Mandatory fields are marked with an asterisk*.

- **e-mail address***: Enter the e-mail address for this receiver in the text field.
- **Subject***: Enter a subject for the e-mail.
- **System Event***: Select the event from the drop-down list for which this receiver is to be notified.

You can add additional System Event Receiver by clicking on the + icon. It is possible to delete System Event Receiver by clicking on the delete 🗑 icon.

Add Cron expression
To be able to receive mail notifications collectively for multiple events within a time interval the messenger allows you to define cron expressions. Click on the "*Add Cron Expression*" button. Mandatory fields are marked with an asterisk*.

- **Cron expression***: Allows to manually set a standard unix "cron expression" to define the email scheduling. Cron expressions are described at http://en.wikipedia.org/wiki/CRON_expression
  It is not possible to specify a day of the month and a day of the week at the same time.

⚠️ **Cron expression syntax**
Please note that the syntax of the cron expression in the X/P Messenger is made of six fields (see below) which represent the time to execute the command.

```
#  ┌──────────────────── second (0 - 59)
#  │  ┌──────────────────── minute (0 - 59)
#  │  │  ┌──────────────────── hour (0 - 23)
#  │  │  │  ┌──────────────────── day of the month (1 - 31)
#  │  │  │  │  ┌──────────────────── month (1 - 12)
#  │  │  │  │  │  ┌──────────────────── day of the week (0 - 6) (Sunday to Saturday;
#  │  │  │  │  │  │                     7 is also Sunday on some systems)
#  │  │  │  │  │  │
#  │  │  │  │  │  │
#  *  *  *  *  *  *  <command to execute>
```

- **Maximum notifications per e-mail**:* The maximum number of notifications per transmitted eMail can be defined. As a result there will be multiple eMails created if the limit per transmission is reached.

You can add additional **Cron expressions** by clicking on the + icon. It is possible to delete Cron Expressions by clicking on the delete 🗑 icon.

11.4. Enter Communication settings

Under **General Configuration** you can specify several additional settings, mandatory fields are marked with an asterisk*.

- **Retransmission Handling:** you can use this setting to specify the number of *Retries **(retransmission attempts) and the *Retry Interval** (in seconds) between attempts. If a message cannot be transmitted successfully in the specified number of retries, the Messenger will give up and mark the message as "failed".
- **Message ID Domain**:* this will be used as suffix when message IDs are automatically generated.
- **SSL Server certificate check:** if you enabled this option only communication with servers, that use SSL certificates that have been issued by a trusted CA known to your Messenger are

allowed. Additionally this setting enables the daily check of server certificate for revocation against the corresponding CA. There for the server certificates are stored for later revocation check. The following behavior is identical to "Partner certificate revocation check" (see below).

- **Allow loopback:** makes it possible to send messages from a Local Partner to another Local Partner.
- **Requeue failed messages:** if you enable this option the messages which could not be transmitted successfully (TTL expired) to the partners shall be re-inserted into the outbound queue. Thus enabling the Messenger to automatically retry the transmission of these messages. [Info Icon] If the receiver did not accept the initial message due to it's large size, then the messenger will not retry sending such messages.
- **Partner certificate revocation check**: If enabled each partner certificate and SSL client certificate is checked once per day against the corresponding CA to ensure it is still valid and wasn't revoked. If CA couldn't be reached properly, the existing certificate will still be treated as valid and will be re-checked the next day. After three days of unsuccessful communication a certificate will be treated as INVALID and won't be used anymore.
- **Ping-ALL:** if this option is enabled the Messenger sends ebXML or AS4 Pings for all Agreements with activated Ping-All option and for all defined URLs (primary and fallback). The results can be queried with the JMX interface. During communication failures (TTL expired) the messenger switches to the defined fallback URI in the agreement if the partner is unreachable via the primary URI.
- **Ping-All Interval (minutes):** defined time intervals to check if the communication partner is reachable.
- **Default Adapter:** defines the default adapter which will be used during agreement creation.

If your Messenger will be connecting to the Internet via a proxy server you must enable HTTP Proxy and/or FTP Proxy.

> [Info Icon] If you are using a PONTON X/P Listener you have the option of using the Listener as a HTTP Proxy for outgoing messages, please see Listener Configuration and Certificates.

Enable HTTP Proxy Configuration

Mandatory fields are marked with an asterisk*.

- **Host**:* Enter the IP address or hostname of your HTTP proxy server.* *
- **Port**: * Enter the port number of your HTTP proxy server.
- **Username/Password:** Enter user/password to be used.
- **NT Domain:** The NT Domain is only required if your proxy server uses NTLM authentication.
- **Bypass Proxy for:** Enter hostname(s) that should not use the HTTP proxy server. Additional hostnames can be added via the + icon.

Enable FTP Proxy Configuration

Mandatory fields are marked with an asterisk*.

- **Host**:* Enter the IP address or hostname of your FTP proxy server.* *
- **Port**:* Enter the port number of your FTP proxy server.
- **Username/Password:** Enter user/password to be used.

Enable LDAP Proxy Configuration

> [Info Icon] If you are using the PONTON X/P Messenger for AS4-BDEW market communication, you have the option of using the Listener as a HTTP Proxy for outgoing LDAP connections required for AS4 certificate handling.

Mandatory fields are marked with an asterisk*.

- **Host***: Enter the IP address or hostname of your LDAP proxy server.
- **Port***: Enter the port number of your LDAP proxy server.

11.5. Enable Time Server

PONTON X/P need to use a correct time setting to ensure trouble-free exchange of Messages and business transactions. The standard solution for this issue is to synchronize the local system time with a time server. There are many high-precision time servers – so-called NTP servers – that can be accessed on the Internet. In general, communication between applications and NTP servers is carried out via UDP packets on port 123. Time synchronization can be carried out at operating system level, or at application level.

> ⚠ If the computer that hosts the Messenger application already has automatic time synchronization at system level, it is recommended to disable the Time Server feature.

Depending on your requirements, you can activate/deactivate the Messenger's Time Server synchronization by selecting/de-selecting the "*enabled*" checkbox. Mandatory fields are marked with an asterisk*.

- **NTP Server:** Enter the NTP server IP or name
- **Synchronize Interval**:* This defines how often the application will synchronize with the NTP server(s) – when enabled. The default setting is to synchronize every 24 hours.

You can add additional **NTP Server** by clicking on the + icon. It is possible to delete NTP Server by clicking on the delete 🗑 icon.

11.5.1. Enter Server settings

11.5.1.1. Connectors

You can add additional Connectors by clicking on the + icon. It is possible to delete Connectors by clicking on the delete 🗑 icon. Mandatory fields are marked with an asterisk*.

- **Protocol**:* Select the protocol (HTTP/HTTPS) you want to use from the drop-down list
- **Port**:* Enter the Port you want to use
- **Service**:* This defines what Services will be available on the port:
  - LISTENERS: allows to received inbound HTTP messages
  - ADAPTER_SERVICE: communication interface for external adapters
  - GUI: old web-GUI (does not have an effect)
  - REST: provides an REST API and also the new web-GUI
  - HTTP_ADAPTER: activates a HTTP Adapter instance (see chapter **Http Adapter** for configuration details)

You can add additional **Services** by clicking on the + icon. It is possible to delete Services by clicking on the delete icon.

[Info Icon] You can define multiple connectors for the communication with the Messenger. A connector specifies the protocol and the port for one or multiple services.

11.5.2. Enter Archive settings

11.5.2.1. Archiver Type

- **NONE** - Nothing will be archived
- **FILE_SYSTEM** - Archiver will use the File System.
- **WEB_SOCKET** - Archiver will use the an Adapter that supports archiving.
- **DATABASE** - Archiver will use the currently configured database.

11.5.2.2. Adapter Id

Only enabled and mandatory when Archiver Type is **WEB_SOCKET**, use this adapter for archiving

11.5.2.3. Archive Folder

Only enabled and mandatory when Archiver Type is **FILE_SYSTEM**

- **Archive Folder**:* Setting can be used to indicate the location of the archiving folders. These can be expressed either as an absolute path to the required folder or a relative path beginning with '$PONTONXP_HOME' – this placeholder refers to the folder [installation root]\data.
- **Archive Failed Folder**:* You can define a separate folder, which will be used to store failed messages. If you prefer to store all your data in a single archive, you can use the same path setting as the Archive Folder.
- **Use Zip Compression:** Enable Zip Compression to reduce the space of the archive on disk.

11.5.2.4. Archivable Message Parts

Select which information should be archived in the a dedicated directory. Each part is stored in a separate file. Each of the listed parts of a message can be archived. You can enable or disable the archiving service for each part by activating/deactivating the corresponding checkboxes.

- **Backend Envelope**
- **Packaging Envelope**
- **Payload – this is the actual business document**
- **Certificate**
- **Signature**
- **Attachment**

11.5.2.5. Archive Cleanup

Files older than the maximum age will be deleted from the filesystem as long as "Delete archive entries" is enabled.

- **Delete archive entries**: Enabled deletion of old archive data.
- **Cleanup Time**:* Deletion of files from the file system will start at the specified cleanup time. [Info Icon] If no value for the cleanup time is set and deletion is activated the messenger will automatically start the cleanup at 03:00:00 Hours. This is a mandatory field.
- **Maximum runtime of Cleanup-Job (minutes)**: The Cleanup-Job will stop, when this maximum runtime (in minutes) is reached and will continue at configured cleanup time the next day
- **Maximum age (days)**:* The number of days specified here will define the maximum number of days the message releated information is retained in the filesystem. This is also a mandatory field.

> ⚠️ **Maximum age**
> It is recommended to define a lower value for the Maximum Age of the Archive Cleanup than the Maximum Age of the Database Cleanup!

11.5.3. Maintenance periods

Click on "Add maintenance period" to enable maintenance which requires to set up at least one maintenance period. Maintenance is used for disable message exchange with all remote partners.

- **From:** Start of maintenance period
- **To:** End of maintenance period
- **Stop delivery to adapters**: incoming messages remain in the inbound queue and will not be sent to adapters.
- **Stop delivery to partners:** outgoing messages remain in the outbound queue and will not be sent to partners.

- **Rejection of incoming messages:** No messages from partners are accepted by the Messenger. The sender will receive an error response.
- **Rejection of outgoing messages:** No messages from the backend adapters are accepted by the Messenger. The adapter will receive an error response.

11.5.4. Enter Listener Connection settings

Selecting "*enabled*" will allow you to enter the Listener connection settings. Mandatory fields are marked with an asterisk*.

- **IP Address Listener**:* Enter the IP address for the Listener connection (Messenger to Listener).
- **Port**:* Enter the port for the Listener connection (Messenger to Listener). The standard port number for this connection is 9000
- **Data connection count**:* The Data connection count refers to the number of parallel communication channels between Listener and Messenger. This number also limits how many simultaneous message transmissions are accepted by the Listener. As per default this is set to 3, but can be increased up to 25.
- **SSL:** SSL is enabled by default. In case you set InternalCommunication.UseSSL=false in your Listener.properties then you have to disable SSL on this page as well. The Listener will only accept connections from known Messenger instances which are listed in the ListenerConfiguration\config\authorization.txt file in the Listener installation.

> ⚠️ **First Connection**
> The first connection from a Messenger instance to a freshly installed Listener will always be accepted by the Listener!

> [Info Icon] **Messenger Instance ID**
> While testing the connectivity between a Listener and a Messenger please make use of the ListenerInstallation\logs\listener.log where the incoming connections from the Messenger including its instance ID are logged.

11.5.5. Enter Adapter API v2 settings

In this section you can enable or disable the adapter api v2 settings. Mandatory fields are marked with an asterisk*.

- **IP Address***: Enter the IP address for adapter api connection.
- **Port***: Enter the port for the adapter api connection. The standard port number for this connection is 2600.
- **Idle timeout (seconds)***: Enter the idle timeout for the adapter api v2 in seconds. Default is 60 seconds.

11.5.6. Authentication Token

The following security settings can be configured:

- **Random secret at restart:** When enabled restarting will invalidate all sessions requiring to log in again.
- **Ignore IP address:** If disabled a given session will only work from the IP address it was started with. Switching to another network during an active session therefore requires logging in again.
- **Expiration time:** This is the time in minutes a session is valid. After this amount of inactivity the GUI automatically ends the session and invalidates the authentication token. The session will not terminate if the GUI is permanently interacted with. An application using the REST-API will have to perform this token refresh manually.

11.5.7. Display

- **Messenger name:** The messenger name displayed in the top navigation bar can be changed. Type in the desired name and click on save.
- **Color adjustment:** Grab and hold (left mouse click) the dot and move the dot to the right side in order to change the color of the top navigation bar. When the desired color has been selected click on save. Alternatively you can type in a number from 0 (default) to 359 in order to vary the color.
- **Environment:** The messenger can be set in either TEST or PRODUCTION mode. Default mode is PRODUCTION. By choosing either of the two modes the messenger automatically selects property values corresponding to the respective modes. The environment relevant properties are usually provided by Config Patch containing the values required for the case specific set up. ⚠️ Messenger must be restarted after the mode change.

11.6. Server certificate

This page allows you to request, install, export and delete certificates for your server. You need those certificates to be able to receive messages via HTTPS when no Listener is used.

When you have received the SSL certificate, open the "*Install Server Certificate*" Dialog by clicking on the Install Certificate 🔧 icon. Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the ⊗symbol. If the file is valid and you have entered a password for the private key you can click on the "*Install*" button to add this Server certificate to your Messenger configuration. When the installation was successful the new Certificate will appear in the Server Certificates list.
[Info Icon] Although a valid TLS certificate (as per BSI PKI_Certificate_Policy_v1.1.2) can be installed as a server certificate here, this is currently not supported for incoming TLS communication.

11.6.1. Request Server certificate

Click on the request new certificate + icon which opens the request certificate dialog box. Fill in the certificate request form. The mandatory fields are marked with an asterisk*:

- **Certificate Name***
- **SAN Value** (subject alternative name)*
- **Organisation***
- **E-mail address***
- **Country*** (select)
- **Key pair*** (select)
- **Private key password***
- **Repeat password***

Optional input fields are: Department; Locality; State or province; Phone number; Fax number. You can also select to build the request with PONTON attributes. You can add additional SAN values by clicking on the by clicking on the + icon. It is also possible to delete a SAN value by clicking on the delete 🗑 icon. Please note that at least one SAN value is required. When you have filled out all required fields the "*Request certificate button*" becomes active.

11.6.2. Request Server Certificate (pre-existing)

Click on the request certificate ◆icon, which appears on the right hand side of the Server Certificate table row when you hoover with your mouse over the Server Certificate for which you want to request a new certificate. On click the request certificate dialog box opens. Fill in the certificate request form. The mandatory fields are marked with an asterisk*:

- **Certificate Name***
- **SAN Value***
- **Organisation***
- **E-mail address***
- **Country*** (select)
- **Key pair*** (select)
- **Private key password***
- **Repeat password***

Optional input fields are: Department; Locality; State or province; Phone number; Fax number. You can also select to build the request with PONTON attributes. You can add additional SAN values by clicking on the by clicking on the + icon. It is also possible to delete a SAN value by clicking on the delete 🗑 icon. Please note that at least one SAN value is required. When you have filled out all required fields the "*Request certificate button*" becomes active.

> ⚠️ **new SSL certificate**
> You need to restart PONTON X/P to let it use the new SSL certificate.

11.6.3. Export Server Certificate

Click on the export icon, which appears on the right hand side of the Server Certificate table row when you hoover with your mouse over the Server Certificate you want to export. When you click on the export icon the Export Certificate dialog will appear. Select either Base64 PEM or Binary DER as format. If you select to "Export the certificate with Private Key" you need to enter the private key password. Clicking on the "*Export*" button will download the Server Certificate to your local folder.

11.6.4. CA Certificates

11.6.4.1. Install Server CA Certificates

When you receive the CA's root certificate as a file (e.g. *.cer) click on Install CA Certificate icon. Either choose a file by clicking on "Choose files" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid click on the "*Install*" button to add this CA certificate to your Messenger configuration. When the installation was successful the new Certificate will appear in the Server CA Certificates list.

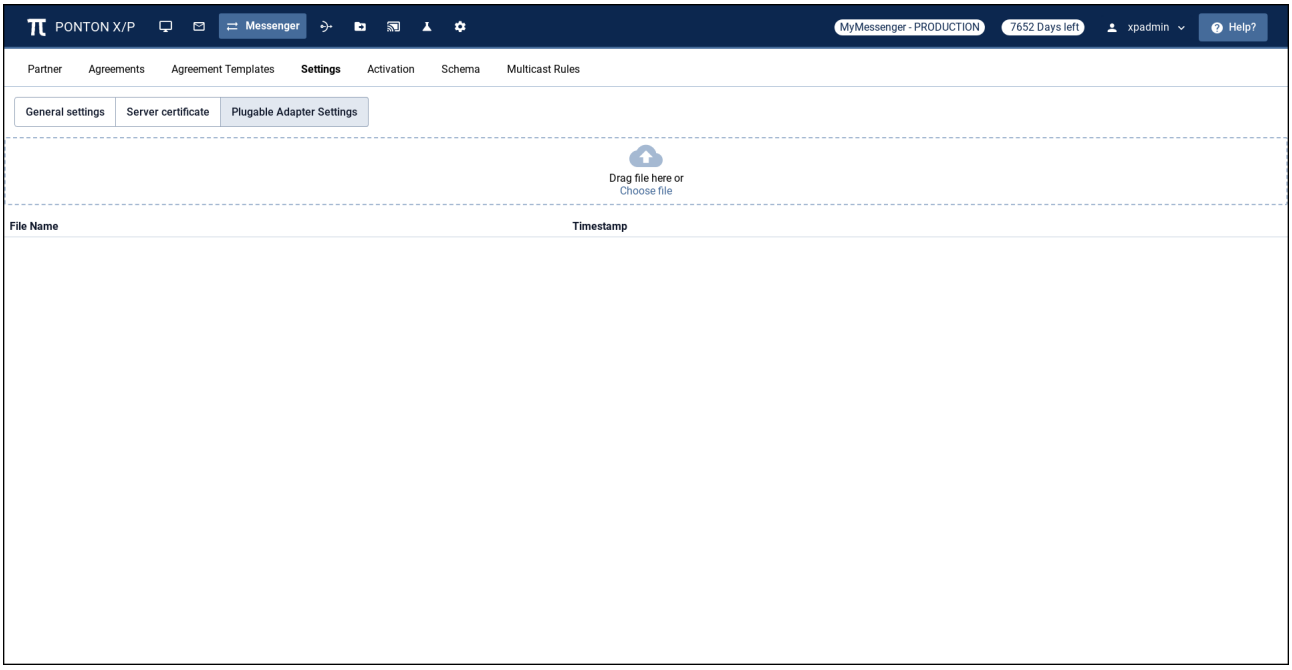
11.6.4.2. Export Server CA Certificates

Click on the export icon, which appears on the right hand side of the Server CA Certificate table row when you hoover with your mouse over the Server CA Certificate you want to export. When you click on the export icon the Export Certificate dialog will appear. Select either Base64 PEM or Binary DER as format. Clicking on the "*Export*" button will download the Server CA Certificate to your local folder.

11.6.4.3. Delete Server CA Certificates

Click on the delete icon, which appears on the right hand side of the Server CA Certificate table row when you hoover with your mouse over the Server CA Certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the Server CA Certificate.

11.7. Plugable Adapter Settings



Manage configuration files that will be used by Plugable Adapters (properties files, keystores etc). Normally the properties file share the name of the adapter, for example "*bwa.properties*"

- The uploaded files requires a Messenger restart to take effect, including another cluster nodes if available.

11.7.1. Upload configuration file

Drag a file or click on the cloud icon to store a file permanently. Already stored file with the same name will be overwritten.

11.7.2. Download configuration file

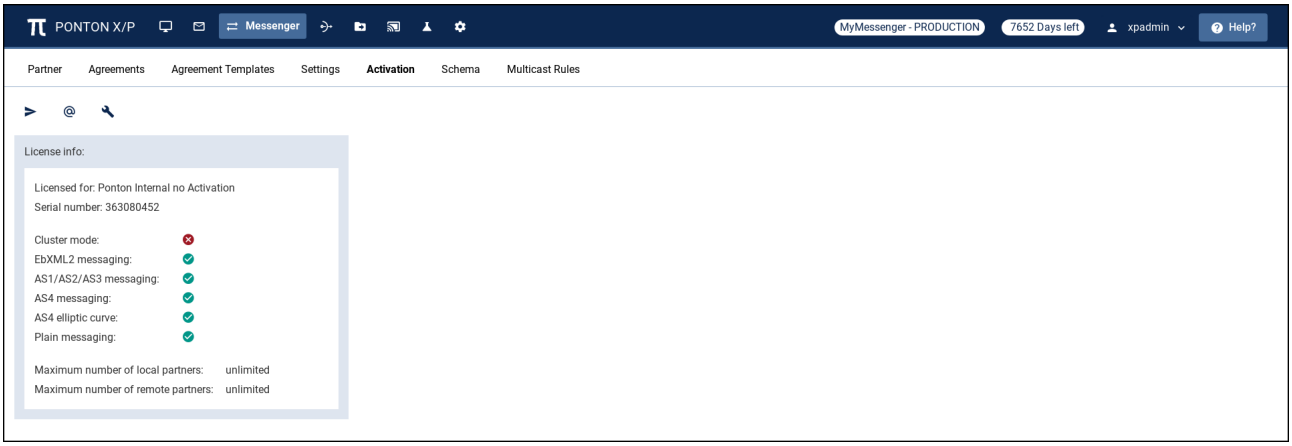
Click the download icon on the table row to download the file to perform required changes, then re-upload the file if needed.

11.7.3. Delete configuration file

Click the delete icon on the table row to delete the stored. The file will be removed from the messenger classpath on the next restart.

12. Messenger >Activation

Go to: **MESSENGER *** ⇄ **> *Activation**



12.1. Get license info

On the Messenger Activation page you can find important information about the PONTON X/P Messenger license. The following details are listed:

- **Licensed for** - license owner
- **Serial Number** - license serial number
- **Cluster Mode** - true, if cluster mode is allowed
- **EbXML2 Messaging** - true, if EbXML v2 messaging is allowed
- **AS1/AS/AS3 Messaging** - true, if AS1/AS2/AS3 messaging is allowed
- **AS4 Messaging** - true, if AS4 messaging is allowed
- **AS4 elliptic curve** - true, if elliptic curve algorithms can be used in AS4 Messaging
- **Plain Messaging** - true, if plain messaging is allowed
- **Maximum Number of Local Partners** - limitation for own partners
- **Maximum Number of Remote Partners** - limitation for communication partners

if no license is installed, then this page will display the limitations of the trial license.

> [Info Icon] The following chapters describes how to install and activate licenses for PONTON X/P. Please note that direct activation via HTTP is not available for trial licenses (included with the software distribution). To activate a trial version you will have to send the activation request by e-mail. Please go to the Initial Setup chapter for more information.

12.2. Send Activation Request

Depending on your license conditions it may be necessary to activate your license after it is installed. To complete your license activation click on the send ➤ icon. This will activate the

license almost immediately. If the license was successfully activated the updated license name e.g. Licensed for: PONTON GmbH is displayed in the under license info on the activation page and the remaining lifetime of the license is displayed on the right side of the navigation bar. e.g. Days left: 1096.
The activation by HTTP will only work if the PONTON activation server (the default URL is https://xpactivation.ponton.de/webactivation/HttpListener) is reachable from the Messenger server. Otherwise please use the activation by e-mail.

12.3. Mail the Activation Request

To submit your activation request by e-mail, click on the mail request @ icon and click on the "*Copy to clipboard*" which copies the complete activation request text in the dialog box to your clipboard. Create a new e-mail with your preferred e-mail client and paste the content in the e-mail. Send the e-mail to activation@ponton.de.

[Info Icon] **Notes**
When sending your activation request by e-mail, make sure activation request code is complete and includes the lines "----- BEGIN ACTIVATION REQUEST -----" and "----- END ACTIVATION REQUEST -----".

12.4. Install activation/license

12.4.1. Installing a license activation

If you have submitted a license activation request via e-mail you will receive a reply containing your activation code. Click on the install license icon and paste the activation code into the text box "**Paste activation or license here**". Make sure that the activation code is complete and includes the lines "----- BEGIN ACTIVATION -----" and "----- END ACTIVATION -----". Click on the "*Install*" button to install the activation. Following the activation the updated license name e.g. Licensed for: PONTON GmbH is displayed in the under license info on the activation page and the remaining lifetime of the license is displayed on the right side of the navigation bar. e.g. Days left: 1096

[Info Icon] **New activation**
Depending on your license conditions, you may need to repeat the license activation process after making certain changes to your own partner configuration.

12.4.2. Installing a license

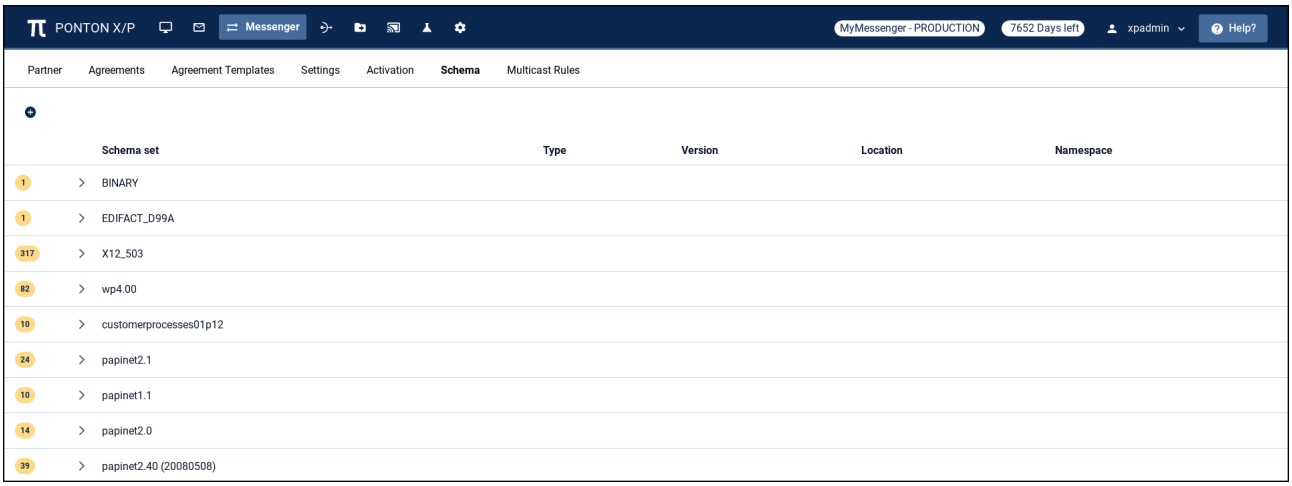
You will generally receive your Ponton X/P license as a text or e-mail from PONTON GmbH or from your licensing organization. To install your license click on the install license icon and paste the license code into the text box "**Paste activation or license here**". Make sure that the license code is complete and includes the lines "----- BEGIN LICENSE -----" and "----- END LICENSE -----". Click on the "*Install*" button to install the license.

13. Messenger >Schema

Go to: **MESSENGER** ⇄ > **Schema**

13.1. View available Schema Sets

The schema set table displays a list of all available Schema Sets. The number in the first column displays how many Message types are available in that specific Schema Set. You can expand the table rows by clicking on the fold/unfold icon › before the Schema Set name. When you expand the Schema Set you will see entries for the Type, Version, Location and Namespace headings.



> ⚠ **Activating Schema Sets**
> The Messenger distinguishes between available Schema Sets and activated Schema Sets. Just inserting entries in the schema configuration, as described in this section, does not activate the Schema Sets or the corresponding schema's for use by the Messenger. In order to make use of the schema's in a Schema Set, you have to activate the Schema Set in the Local Partner configurations > **Schema Sets** section (or Remote Partner configuration >**Schema Sets**) and the agreements configuration >**Schema Set** section

13.2. Import a new Schema Set

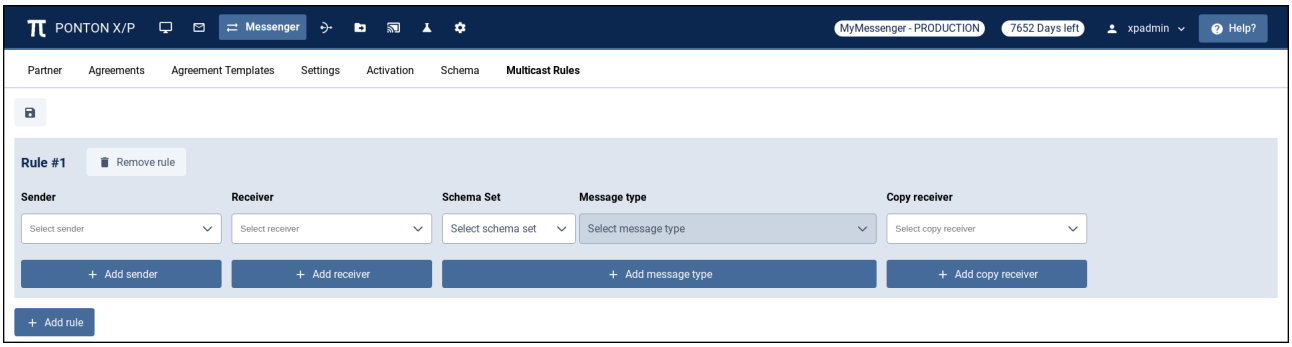
Click on the plus ⊕ icon (top left) to import a new Schema Set which opens the "*Upload Schema Set*" dialog box. Either choose a file by clicking on "Choose files" or drag-and-drop a valid file into the marked area. Only ZIP files containing .dtd .xsd and .xml files are accepted by the GUI. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the ⊗ symbol. When the file is valid you can click on the "*Upload Schema Set*" button to start the upload process. When the upload was successful the new Schema Set will appear in the Schema Set list.

14. Messenger >Multicast Rules

Background:

Multicast rules allow the sender of a message to send duplicates of certain messages to additional receivers (copy receiver). Messages for which multicast rules apply must specify an receiver and copy receiver as well as Schema Set and Message Type. Duplicated messages are shown in the Message Monitor and can be processed like any other messages. The conversation ID of duplicated messages is identical with the conversationId of the original message, while the MessageIds of the duplicated messages is derived from the original MessageId. If the original message had a filename defined, it is also set in the duplicated message.

In order to set up multicast rules go to: **MESSENGER** ⇄ > **Multicast Rules**



Click on the + Add Rule button to add a new role which opens the "*Rule #1*" for the first rule. Just click on the + Add Rule button again if you would like to set up another rule. There are no limits on how many rules you can add.

- **Sender**: Sender who is creating the Message in his backend
- **Receiver:** Receiver of the original Message who is responding with an acknowledgement (ACK) Message
- **Schema Set**: Schema set for which the created rule applies
- **Message Type:** Message Type within a Schema Set for which the rule applies
- **Copy Receiver:** The receiver of the duplicated message. The acknowledgement for a duplicated message appears in the XP Messenger but is not passed to the backend of the Sender.

You must select at least one of each criteria above for a valid rule. You can add additional values for Sender, Receiver, Messages Types and Copy Receiver by clicking on the + **Add...** button. When selecting multiple senders, receivers or message types a match on any of them will trigger a copy to all the copy receivers.

Click on the save icon 💾 to save the completed rule. In order to remove a rule click on the 🗑 Remove Rule button.

15. Listener Configuration and Certificates

Go to: *LISTENER * 

The Listener configuration enables you to specify the Listener configuration in a distributed installation.

15.1. Listener Configuration

To securely receive messages it is recommended to use the PONTON X/P Listener. The Listener can run on a computer in the DMZ, separate from the Messenger. The purpose of the Listener is to accept incoming connections and forward the data to the Messenger (across the firewall). The firewall rules must be set up to allow a connection from the Messenger to the Listener.

⚠️ If you are going to receive messages via the Listener, your partners will have to enter the public URI of your Listener in their configurations (under **MESSENGER** ⇄ → Partners → My Partners → <select partner> → Communication Tab → URI of Partner's Messenger Service).

[Info Icon] **Listener installation**
You also have the option of subsequently installing the Listener as a service under Windows – this service can then be configured to start automatically when the system starts up. The service installer lies directly underneath the main listener folder after unpacking.

15.1.1. Proxy Settings

Enable or disable the use of the Listener as a HTTP proxy server for outbound connections.

- **IP Address / Port:** Select the IP address and the port on which the HTTP proxy server will be started. Make sure that the firewall allows connections from the Messenger to the HTTP proxy server.

15.1.2. HTTP Settings

Enable or disable the use of the Listener for incoming HTTP and HTTPS connections. The Listener IP address and the port number is used to receive messages from communication partners. If no specific IP address is selected, the incoming connections will be accepted on all available IP addresses on the specified port number.

- **HTTP / HTTPS:** enables the Listener to handle the relevant protocols.
  - In case HTTPS is enabled the following options can be activated:
    - **SNI Enabled:** activate this to require SNI parameter on HTTPS requests. This also requires a HTTPS certificate that contains a SAN matching the hostname of the public URL.
    - **Client certificate check:** specifies that the Listener will only accept HTTPS connections

from clients that provide a known client certificate during HTTPS handshake. These client certificate can be installed under the **Client Certificates** tab. It is activated per default.

  - **Use partner certificates:** specifies that the communication partner certificates installed in your Messenger's partner configurations will be copied to the Listener configuration and used for authentication of incoming HTTPS connections, if the option **Client certificate check (Identity)** is enabled. This also enables automatic synchronization of Partner Certificates between Messenger and Listener. It is deactivated per default.

- **IP Address Listener /Port:** Enter the **IP address** and **port** for incoming connections of the relevant protocol (HTTP or HTTPS).
- **Max. data size:** specifies the maximum size (in bytes) of incoming messages, including the transport envelope. The sender will receive a HTTP error when the message size is too large.

15.1.3. FTP Settings

Enable or disable the use of the Listener for FTP server connections. The data connection IP address and the port number is used to receive messages from communication partners.

- **IP Address Listener /Port**: Enter the **IP address** and **port** for the FTP server.
- **IP Address Data Connection /Port**: Enter the **IP address** and **port-range** for the Data connections. IP and Port are needed for FTP data transmissions. Please make sure that the correct public IP address is provided. The port-range limits how many simultaneous data transmissions can be executed, because each transmission requires a dedicated port.

⚠ When the FTP Listener has used up all data ports (one per data transfer), the next partner will have to wait for a data port to become available.

On the "*Add Logins*" button you can create, delete and edit FTP users and the mapping between FTP user and communication partner.

⚠ **Login details**
You must provide your communication partners with the FTP Login details (Login Name, Password, IP and PORT) so that they can deliver messages successfully to your FTP Listener.

15.2. Listener certificate

The **Listener Certificate** tab provides an overview of the installed Listener Certificates (SSL Server Certificate) for HTTPS or FTPS connections. The CA certificates belongs to the Listener certificates. In case you have assigned different URLs to different local partners in your Messenger and you are using the Listener for inbound communication, then you are required to install the TLS certificates of all the required local partners on the listener machine individually.

15.2.1. Install Listener Certificate

Open the Install Listener Certificate Dialog by clicking on the Install Certificate icon . Either choose a file by clicking on "Choose files" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid and you have entered a password for the private key you can click on the "*Install*" button to update the Listener Certificate. When the installation was successful the new Certificate will appear in the Listener Certificates list.

15.2.2. Request Listener Certificate

Click on the request certificate icon, which appears on the right hand side of the Listener Certificate table row when you hoover with your mouse over the Listener Certificate for which you want to request a new certificate. On click the request certificate dialog box opens. Fill in the certificate request form. The mandatory fields are marked with an asterisk (*):

- **Certificate Name; SAN Value, Organisation; E-mail address**
- **Country (select); Key pair (select)**
- **Private key password**
- **Repeat password**

Optional input fields are: Department; Locality; State or province; Phone number; Fax number. You can also select to build the request with PONTON attributes. You can add additional SAN values by clicking on the by clicking on the + icon. It is also possible to delete a SAN value by clicking on the delete icon. Please note that at least one SAN value is required. When you have filled out all required fields the "*Request certificate button*" becomes active.

15.2.3. Request Listener Certificate (with new SAN values)

Click on the request certificate + icon and a request certificate dialog box opens. Fill in the certificate request form. The mandatory fields are marked with an asterisk (*).

> ⚠️ **Overwriting Requests**
> While requesting multiple listener certificates one after another, please note, that new requests overwrite previous server certificate requests. Installing a server certificate requires that the corresponding request is also available. Thereby, it is recommended to request and install the server certificates in a chronological manner.

15.2.4. Export Listener Certificate

Click on the export icon , which appears on the right hand side of the Listener Certificate table row when you hoover with your mouse over the Listener Certificate. When you click on the export icon the "*Export Certificate*" dialog will appear. Select either Base64 PEM or Binary DER as format. If you select to "Export the certificate with Private Key" you need to enter the private key password. Clicking on the "*Export*" button will download the Listener Certificate to your local folder.

15.2.5. Install Listener CA Certificate

Open the Install Listener CA Certificate Dialog by clicking on the Install CA Certificate icon. Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid you can click on the "*Install*" button to add this Listener CA certificate to your Listener configuration. When the installation was successful the new CA Certificate will disappear in the Listener CA Certificates list.

> ⚠ **Pre-installed CA certificate**
> The PONTON CA certificate is preinstalled, so you will not need to install a CA certificate if you use certificates issued by PONTON.

15.2.6. Export Listener CA Certificate

Click on the export icon, which appears on the right hand side of the Listener CA Certificate table row when you hoover with your mouse over the Listener CA Certificate you want to export. When you click on the export icon the "*Export Certificate*" dialog will appear. Select either Base64 PEM or Binary DER as format. Clicking on the "*Export*" button will download the Listener CA Certificate to your local folder.

15.2.7. Delete Listener CA Certificate

Click on the delete icon, which appears on the right hand side of the Listener CA Certificate table row when you hoover with your mouse over the Listener CA Certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the Listener CA Certificate.

15.3. Client Certificates

The client certificates tab provides an overview of all your client certificates, which are used for the authentication of HTTPS connections. The currently installed Client Certificates are shown in the Client certificates table.

15.3.1. Install Client Certificate

Open the Install Client Certificate Dialog by clicking on the Install Certificate icon. Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid click on the "*Install*" button to add this Client certificate to your Listener configuration. When the installation was successful the new Certificate will disappear in the Client Certificates list.

15.3.2. Export Client Certificate

Click on the export icon, which appears on the right hand side of the Client Certificate table row when you hoover with your mouse over the Client Certificate you want to export. When you click on the export icon the "*Export Certificate*" dialog will appear. Select either Base64 PEM or Binary

DER as format. Clicking on the "*Export*" button will download the Client Certificate to your local folder.

15.3.3. Delete Client Certificate

Click on the delete icon, which appears on the right hand side of the Client Certificate table row when you hoover with your mouse over the Client Certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the Client Certificate.

15.3.4. Install Client CA Certificate

When you receive the CA's root certificate as a file (e.g. *.cer) click on Install CA Certificate icon. Either choose a file by clicking on "*Choose files*" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. If the file is valid click on the "*Install*" button to add this CA certificate to your Listener configuration. When the installation was successful the new CA Certificate will disappear in the Client CA Certificates list.

15.3.5. Export Client CA Certificate

Click on the export icon, which appears on the right hand side of the Client CA Certificate table row when you hoover with your mouse over the Client CA Certificate you want to export. When you click on the export icon, the "*Export Certificate*" dialog will appear. Select either Base64 PEM or Binary DER as format. Clicking on the "*Export*" button will download the Client CA Certificate to your local folder.

15.3.6. Delete Client CA Certificate

Click on the delete icon , which appears on the right hand side of the Client CA Certificate table row when you hoover with your mouse over the Client CA Certificate you want to delete. When you click on the delete icon a confirmation dialog opens, Clicking on the "*Yes*" button will delete the Client CA Certificate.

[Info Icon] **CA Certificates**
PONTON X/P uses trusted certificates to ensure the identity and authorization of communication partners. PONTON offers its own lightweight certification authority. This is the default CA Certificate in a standard PONTON X/P installation. If you want to use certificates issued by a 3rd party CA you will need to install the root certificate of the CA and all needed intermediate certificates. You will not be able to install partner certificates issued by a given CA until all needed CA certificates have been installed.

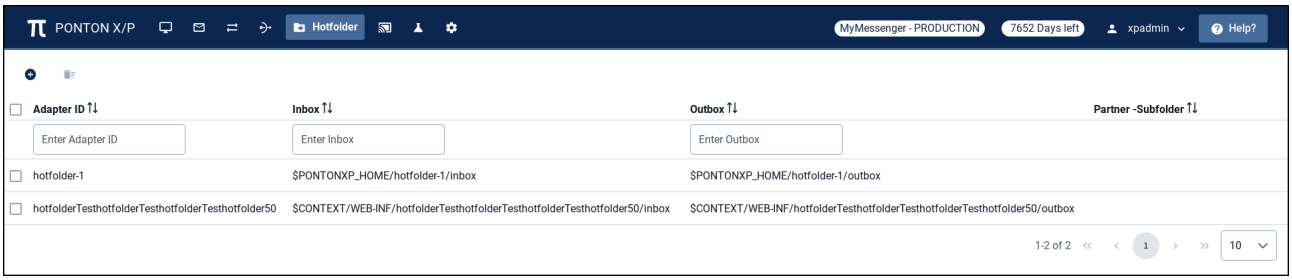
16. Hotfolder

Go to: **HOTFOLDER**

16.1. View available Hotfolder

The **Hotfolder** table displays a list of all created Hotfolders. The following functions are available to easily find the table entry you are looking for:

- All table headings have a **Sort** function (icon). Sort can be ascending and descending.
- Some table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.



16.2. Create a new Hotfolder

Click on the "*Create a new hotfolder*" icon which opens the "Create New Hotfolder" dialog box. Enter a "**New Adapter ID**" in the text box and click on the "*Next Step*" button which opens the **Configuration** page for the new Hotfolder. The Adapter ID you have created is displayed below the sub-navigation bar.

16.2.1. Enter General Settings

Mandatory fields are marked with an asterisk (*****).

- **Work Folder**:* Enter the folder for the Work Folder in the text box either as absolute pathname to the required folder or as relative pathname beginning with '$PONTONXP_HOME' - this placeholder refers to the Messenger's '**data**' folder.
- **Use XML acknowledgement:** If you activate this option, the Hotfolder will store acknowledgements generated by Messenger for every outgoing message in the specified folder.
- **XML Acknowledgement Inbox**:* Enter the folder for your Acknowledgement Inbox in the text box using an absolute or a relative pathname.

[Info Icon] Variables can also be used to define (Ack-)Inbox-paths. The example below shows how inbox paths can be specified using variables.

Inbox path configuration	**(Example) Filename created in the Inbox**	**Hint**
$PONTONXP_HOME\TEST-HF\inbox\File_%test_flag%\%sender%	...\inbox\File_Test\EIC-CODE	• This folder will only **be created once anincoming messagehas been received by the hotfolder** • %sender% describes the sender of the incoming message • %receiver% describes the receiver of the incoming message

16.2.2. Enter Inbox Settings

Mandatory fields are marked with an asterisk (*****).

- **Inbox Folder**:* Enter the folder for your incoming Messages in the text box either as absolute pathname to the required folders or as relative pathname beginning with '$PONTONXP_HOME' - this placeholder refers to the Messenger's '**data**' folder.
- **Filename Pattern**:* Enables you to define individual filenames for the incoming files processed by the Hotfolder Adapter and individual folder structures while saving incoming messages and acknowledgements. The file name of incoming messages is defined by a naming scheme. The naming scheme is determined once per Hotfolder instance. The naming scheme consists of static and dynamic components. The dynamic components are represented as variables (please see the table bellow).
- **Max. number of parallel inbound messages***: Enter a value specifying the maximum number of messages, that this Hotfolder Adapter should be able to receive in parallel.
- **Save BackEnd Envelope:** If you activate this checkbox, the Hotfolder Adapter will wrap **XML** payloads with a BackEnd Envelope containing meta data of the transmission.
- **Support attachments:** If this option is activated, the Hotfolder Adapter will save any files attached to an incoming message into the selected inbox.

Following parameter values are supported as Filename patterns in the Hotfolder:

Variable	**Type**	**Description of this value**
%database_id%	Integer	Database ID of an incoming message.
%message_id%	Text	Message ID as defined by the sender.

Variable	Type	Description of this value
%conversation_id%	Text	Conversation ID as defined by the sender.
%sender%	Text	Backend Partner ID of the sender in the local Messenger.
%receiver%	Text	Backend Partner ID of the receiver in the local Messenger.
%message_type%	Text	Message Type as recognised by the Messenger. This depends on the activated SchemaSets (and Message Types) as well as the agreement configuration in the Messenger.
%schema_set%	Text	SchemaSet as recognized by the Messenger. This depends on the activated SchemaSets (and Message Types) as well as the agreement configuration in the Messenger.
%timestamp%	Integer	Latest timestamp corresponding to the processing timestamp in the Hotfolder.
%test_flag%	Text	"Test" or "Production" depends on whether the Testflag is activated in the message or not.
%original_filename%	Text	The Filename without extension as sent by the sender of this message.
%default_extension%	Text	File extension determined by the Messenger for the received message content (payload).
%original_extension%	Text	File extension as sent by the sender of this message.
%processing_directive_<PROCESSING_DIRECTIVE>%	Text	Replace <PROCESSING_DIRECTIVE> with the needed processing directive. [Info Icon] The supported processing directives can be found in the backend envelopes of the transmitted messages.

A list of widely used filename patterns can be seen in the table below:

Example: Filename pattern configured in the messenger	Example: Result of the filename on the filesystem	Comment
payload-id-%database_id%.%default_extension%	payload-id-123.xml	[Info Icon] This is the default hotfolder setting
BEGIN_%database_id%_%sender%_END	BEGIN_7654321_EIC-CODE_END	The incoming message will be saved on the filesystem without any extension, as there is none defined
%message_id%.%default_extension%	MID-1234.xml	%default_extension% as recognised by the messenger for the incoming message type and schemaset

Example: Filename pattern configured in the messenger	Example: Result of the filename on the filesystem	Comment
%conversation_id%.%default_extension%	Con-1234.edi	As more than one incoming messages can have identical conversation IDs saving such duplicates on the filesystem could cause problems
%timestamp%.%default_extension%	1398778711000.xml	The timestamp corresponds to the time of saving the file on the filesystem as variant time.

16.2.3. Enter Outbox Settings

Mandatory fields are marked with an asterisk (*).

- **Outbox Folder**:* Enter the folder for your outgoing Messages in the text box either as absolute pathname to the required folders or as relative pathname beginning with '$PONTONXP_HOME' - this placeholder refers to the Messenger's '**data**' folder.
- **Failed Folder***: Enter the folder for failed Messages in the text box either as absolute pathname to the required folders or as relative pathname beginning with '$PONTONXP_HOME' - this placeholder refers to the Messenger's '**data**' folder.
- **Use partner subfolders:** If activated, the Hotfolder Adapter will create a separate subfolder in the outbox for each communication partner if an agreement with this partner exists. The name of the folder is the Backend Partner ID of the communication partner.
- **Sender:** If you enable Partner subfolders you must select a fixed sender for all messages from the drop-down list.
- **Scan interval*** (seconds): Enter a value in seconds specifying how often the Hotfolder Adapter should check for new files.
- **Min. file age** (seconds): Define a minimum age in seconds for your files to process. If you like to process files with a minimum age, the Hotfolder can filter your files by file age. The Hotfolder will wait until a given file age is reached and then process the file.
- **Max. number of parallel outbound messages**:* Enter a value specifying the maximum number of messages, that this Hotfolder Adapter should be able to send in parallel.
- **File extension**:* Defines which files should be accepted by the Hotfolder for processing. You can add additional File Extensions if required by clicking on the + icon. It is also possible to delete a File Extension by clicking on the delete 🗑 icon. Please note that at least one File Extension is required.
- **File processing**:* Specifying processing options for outgoing files and allows the Hotfolder Adapter to recognize the type of files regardless of the file extension e.g. XML, BINARY. Processing options help you to define the content of the files which are dropped into the Hotfolder outbox irrespective of their file extensions.

The following table provides an overview of file processing options:

File Extension	Processing option	processing description
• txt • edi • xml • x12	autodetect	[Info Icon] This is the default hotfolder setting Using this configuration of the Hotfolder following result can be expected: • Only 'txt', 'xml', 'x12' and 'edi' Files are picked up from the outbox • Files with other extensions will not be picked up from the outbox • The files will only be processed by the messenger if the following conditions apply ◦ as an XML message ▪ if the content of the 'xml' file can be recognised as a valid XML ▪ and if the Message Type of the message is activated in he Agreement ◦ as a BINARY message ▪ if the file has the extension 'txt' ▪ and if BINARY as Message Type is activated in the Agreement Hint: All formats other than 'xml', 'x12' and 'edi' will be processed as BINARY as long as autodetect is activated
• txt • edi • xml • x12 • png • pdf	Binary	Using this configuration of the Hotfolder following result can be expected: • Only 'txt', 'xml', 'x12', 'png', 'pdf' and 'edi' Files are picked up from the outbox • Files with other extensions will not be picked up from the outbox • The files will only be processed by the messenger if the following condition applies: ◦ BINARY as Message Type is activated in the Agreement

⚠ Outbox Subfolders
In case some older partner subfolders (without an agreement) already exist in your Hotfolder Outbox, please delete those obsolete subfolders manually, so that only the files from valid partner subfolders are collected by the Hotfolder.

⚠ AckInbox Folder
The Acknowledgement Inbox folder as well as Inbox subfolders are only created once incoming Acks or messages are received for the respective partner.

16.3. Delete a Hotfolder

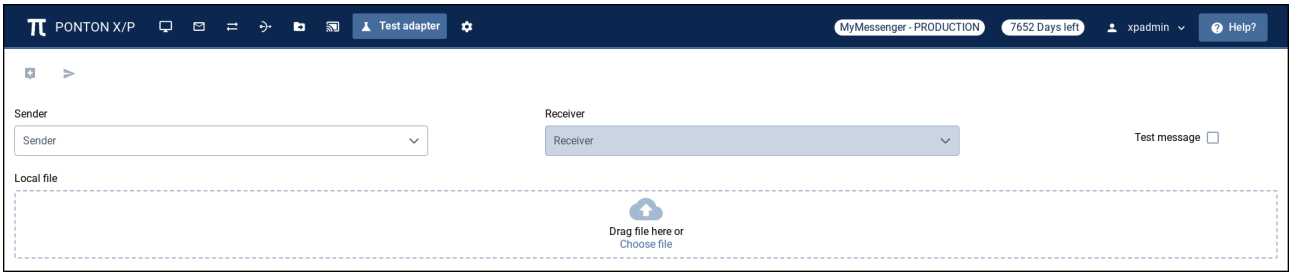
Select one or several Hotfolders by clicking on the checkbox on the left hand side in the table row. The number of selected Hotfolders is displayed next to the delete icon. Click on the delete icon and confirm that you want to delete the Hotfolder.

16.4. Edit a Hotfolder

Select a Hotfolder by clicking on the edit icon which will appear on the right hand side of the table row when you hoover with your mouse over the Hotfolder you want to edit. When you click on the edit icon the Hotfolder **Configuration** page opens, You can go back to the **Hotfolder** page by clicking on the **"Back to Hotfolder"** button or leave the Hotfolder area by clicking on the navigation or sub-navigation bar.

17. Test Adapter

Go to: **TEST ADAPTER**



17.1. Send a Ping message

PONTON X/P Messenger is delivered with a built in Test Adapter. It can be used to send EbXml or AS4 Ping messages to test the connectivity between your own Messenger and your communication partner. Select a sender and a receiver from the drop-down menus. Click on the icon in order to execute a ping from sender to receiver. This will send a Ping message to the chosen receiver. If your Ping message could reach the receiver and he recognizes you as a partner the response should be a **Pong message**. A Pong message does not ensure that your firewall allows incoming messages from your business partner.

17.2. Send a Test Message

To send a test message file to your partner using the test adapter, select a sender and a receiver from the drop-down menus. The drop-down menu for the receiver enables you to search for a partner and select a partner from the returned list (in alphabetical order) of all partners matching the searched letters or name. Enable the Test Message checkbox in case you want to flag the message explicitly as test message. Either choose a file by clicking on "Choose files" or drag-and-drop the file into the marked area. The name and size of the file will appear in the dialog box. You can remove the file by clicking on the symbol. When the file is valid you can click on the send icon.

⚠ The file is processed by your Messenger and will be send to the specified receiver. Only if the processing and packaging settings at the receivers end conform to the settings in your agreement and your network allows transmissions to your communication partner then the message delivery will be successful.

18. Http Adapter

18.1. Configuration

To configure a *HttpAdapter* you must create a new Server Connector under Messenger Settings with only one Service: *HTTP_ADAPTER*

For security reasons a valid Messenger user with the *HTTP-Adapter* role is required to communicate with the HttpAdapter.
NOTE: After a Messenger user is created, log in with the user to change the initial password.

⚠️ Changes of HttpAdapter configuration requires a Messenger restart to become valid.

18.1.1. Documentation Link

After successful configuration of the http adapter the documentation regarding the individual endpoints can be found under the following URL:
Http(s)://<host>:<httpadapter_port>/httpadapter/swagger-ui/index.html

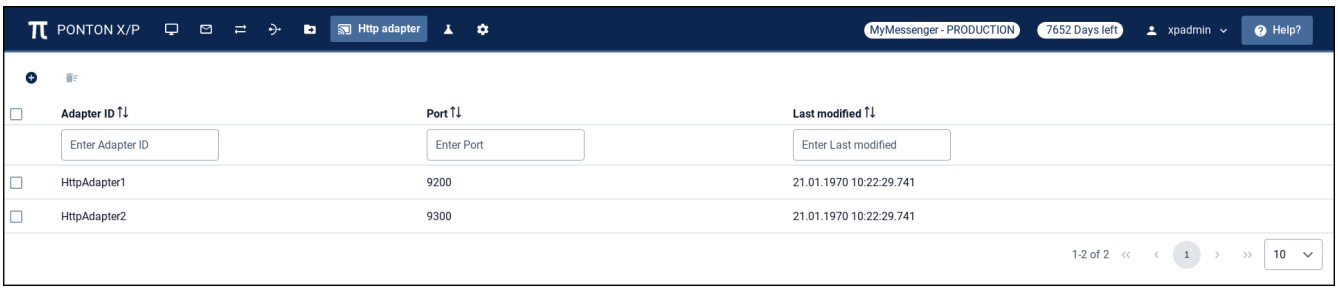
18.1.2. Multiple Http Adapters

It is possible to create multiple HttpAdapters by creating several Server Connectors with unique port numbers.

18.1.3. View available HttpAdapters

The **Http adapter** table displays a list of all created HttpAdapters. The following functions are available to easily find the table entry you are looking for:

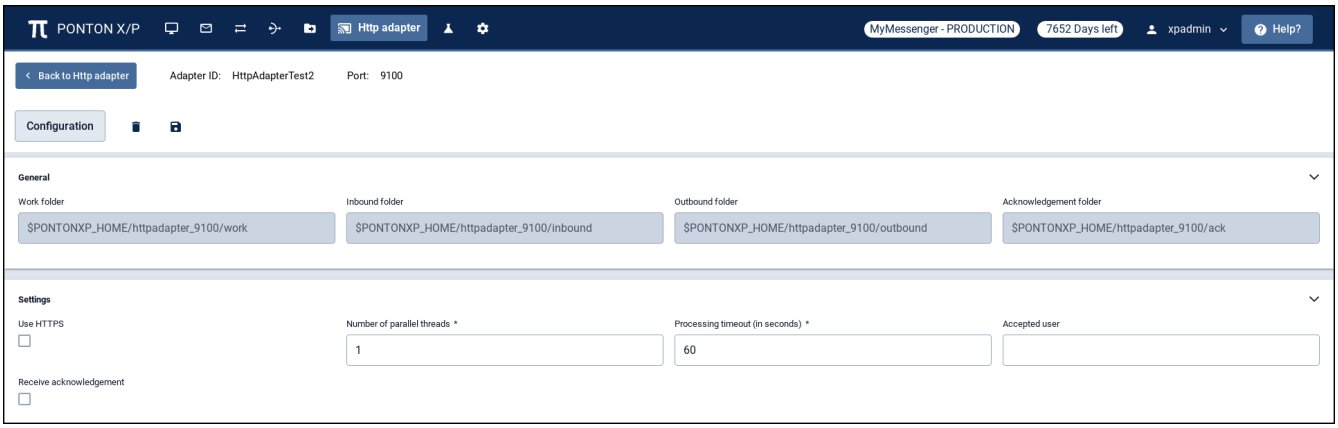
- All table headings have a **Sort** function (icon). Sort can be ascending and descending.
- All table headings have a **Filter** functions. Enter values in the filter text box and the table displays only values which contain the entered filter value. Filters can be combined.
- Underneath the table in the bottom right corner you find a **Pagination** function. The default pagination is 10 entries per page and can be changed to 25 or 50. Up to five pages are displayed in the page toggle bar, you can move forward or backward by clicking on the page number, the forward / backward icons or the first page / last page icon. The active page is highlighted in blue.



18.1.4. Create a new Http adapter

Click on the "*Create a new http adapter*" ⊕ icon which opens the "Create New Http adapter" dialog box. Enter a "**New Adapter ID**" and a "**New Port**" in the text boxes and click on the "*Next Step*" button which opens the **Configuration** page for the new Http adapter. The Adapter ID and Port you have created is displayed below the sub-navigation bar.

> ⚠ The port number has to be the number set in the Server Connector.



18.1.5. Enter General Settings

The folder fields are set automatically and ca not be changed

- **Work Folder**: The folder is used while processing messages.
- **Inbound Folder**: This folder will contain the inbound messages that were not fetched by the backend yet. ⚠ While using an HTTP Adapter in a messenger cluster it is advised to define this path so that it is accessible by all messenger nodes.
- **Outbound Folder**: This folder will store messages that were transmitted from the backend.
- **Acknowledgement Folder**: This folder will contain the acknowledgements for sent messages that were not fetched by the backend yet.
- **Receive acknowledgement**: If the value is true the Http-Adapter will receive acknowledgements for sent messages. Default is false.
- **Use Https**: If the value is true the Http-Adapter will use HTTPS. Default is false.
- **Number of parallel threads**: The value specifying the number of parallel threads for this Http Adapter.
- **Processing timeout (in seconds)**: The value is the maximum time in seconds until processing timout.
- **Accepted user**: If this value is set then only the defined user is authorized to use this Http-Adapter.

18.1.6. Delete a Http adapter

Select one or several HttpAdapters by clicking on the checkbox on the left hand side in the table

row. The number of selected HttpAdapters is displayed next to the delete icon. Click on the delete icon and confirm that you want to delete the Http adapter.

18.1.7. Edit a Http adapter

Select a Http adapter by clicking on the edit icon which will appear on the right hand side of the table row when you hover with your mouse over the Http adapter you want to edit. When you click on the edit icon the Http adapter **Configuration** page opens, you can go back to the **Http adapter** page by clicking on the "**Back to Http adapter**" button or leave the Http adapter area by clicking on the navigation or sub-navigation bar.

18.2. Outbound Direction

To send a message through the HttpAdapter send a *POST* request to *http(s)://<PONTONXP_HOST>:<HTTP_ADAPTER_PORT>/httpadapter/outbound*

- replace <PONTONXP_HOST> with the correct PONTON XP hostname.
- replace <HTTP_ADAPTER_PORT> with the configured port for the HttpAdapter.

18.2.1. Request

The following *HTTP Headers* can be optionally set:

- X-MessageId - use this header to set the Message ID
- X-ConversationId - use this header to set the Conversation ID
- X-SchemaSet - use this header to explicitly set the schemaset of the message
- X-MessageType - use this header to explicitly set the message type of the message
- X-MessageVersion - use this header to explicitly set the message version of the message
- X-BackendSenderId - use this header to explicitly set the Sender Backend ID of the message
- X-BackendReceiverId - use this header to explicitly set the Receiver Backend ID of the message
- X-Filename - use this header to explicitly set filename of the message

Values for the Headers must use ASCII character set.

The *Request Body* must contain the data of the message.

18.2.2. Response

One of the following response codes can be received with the response:

- 204 (OK) - the message was successfully processed by the messenger
- 400 (Failed) - an error occurred while processing the message
- 401 (Unauthorized) - the used user is not accepted by the HttpAdapter

Depending on the response code the following *Request Headers* can be received with the response:

- X-MessageId - the Message ID of the message
- X-ConversationId - the Conversation ID of the message
- X-SchemaSet - the schemaset of the message
- X-MessageType - the message type of the message
- X-MessageVersion - the message version of the message
- X-BackendSenderId - the Sender Backend ID of the message
- X-BackendReceiverId - the Receiver Backend ID of the message

18.3. Receive Acknowledgements for sent messages

Normally for each sent message the messenger delivers an acknowledgment (ACK), wich sent by the receiver.

To receive a next ACK via the HttpAdapter send a *GET* request to *http(s)://<PONTONXP_HOST>:<HTTP_ADAPTER_PORT>/httpadapter/ack*.

- replace <PONTONXP_HOST> with the correct PONTON XP hostname.
- replace <HTTP_ADAPTER_PORT> with the configured port for the HttpAdapter.

18.3.1. Request

The following *HTTP Headers* can be set optionally to ensure that the HTTP Adapter does not delete the incoming ACK file (from the ack_folder) before the backend has accepted the ACK delivery:

- X-DeleteAfterConfirmation - If the value of the header is **true**, the HttpAdapter delivers the same next ACK until the reception of the ACK is explicitly acknowledged by the client (see Request Header *X-LastId*). Otherwise, the HttpAdapter delivers the next ACK without waiting for an acknowledgement.
  When this header does not exist, then no acknowledgement is expected.
- X-LastId - use this header to acknowledge the last successfully received ACK (see Response Header *X-Id*).

Values for the Headers must use ASCII character set.

18.3.2. Response

One of the following response codes can be received with the response:

- 200 (Ok) - the next ACK was successfully transmitted by the HttpAdapter
- 401 (Unauthorized) - the used user is not accepted by the HttpAdapter
- 404 (Not found) - there are no ACKs in the HttpAdapter

The following *Http Headers* are received with the response if the response code is 200:

- X-Id - unique ACK id generated by the Ponton XP

- X-MessageId - the Message ID of the ACK
- X-ConversationId - the Conversation ID of the ACK/sent message
- X-Ref-Id - unique message id generated by the Ponton XP
- X-Ref-MessageId - the Message ID of the sent message
- X-Ref-SchemaSet - the schemaset of the sent message
- X-Ref-MessageType - the message type of the sent message
- X-Ref-MessageVersion - the message version of the sent message
- X-Ref-BackendSenderId - the Sender Backend ID of the sent message
- X-Ref-BackendReceiverId - the Receiver Backend ID of the sent message

The *Response Body* contains the data of the ACK as XpAcknowledgement in XML format.

18.4. Inbound Direction

To receive a next message via the HttpAdapter send a *GET* request to *http(s)://<PONTONXP_HOST>:<HTTP_ADAPTER_PORT>/httpadapter/inbound*.

- replace <PONTONXP_HOST> with the correct PONTON XP hostname.
- replace <HTTP_ADAPTER_PORT> with the configured port for the HttpAdapter.

18.4.1. Request

The following *HTTP Headers* can be set optionally to ensure that the HTTP Adapter does not delete the incoming message file (from the inbound_folder) before the backend has accepted the message delivery:

- X-DeleteAfterConfirmation - If the value of the header is **true**, the HttpAdapter delivers the same next message until the reception of the message is explicitly acknowledged by the client (see Request Header *X-LastId*). Otherwise, the HttpAdapter delivers the next message without waiting for an acknowledgement.
  When this header does not exist, then no acknowledgement is expected.
- X-LastId - use this header to acknowledge the last successfully received message (see Response Header *X-Id*).

Values for the Headers must use ASCII character set.

18.4.2. Response

One of the following response codes can be received with the response:

- 200 (Ok) - the next message was successfully transmitted by the HttpAdapter
- 401 (Unauthorized) - the used user is not accepted by the HttpAdapter
- 404 (Not found) - there are no messages in the HttpAdapter

The following *Http Headers* are received with the response if the response code is 200:

- X-Id - unique message id generated by the Ponton XP
- X-MessageId - the Message ID of the message
- X-ConversationId - the Conversation ID of the message
- X-SchemaSet - the schemaset of the message
- X-MessageType - the message type of the message
- X-MessageVersion - the message version of the message
- X-BackendSenderId - the Sender Backend ID of the message
- X-BackendReceiverId - the Receiver Backend ID of the message
- X-Filename - the filename of the message.

The *Response Body* contains the data of the message.

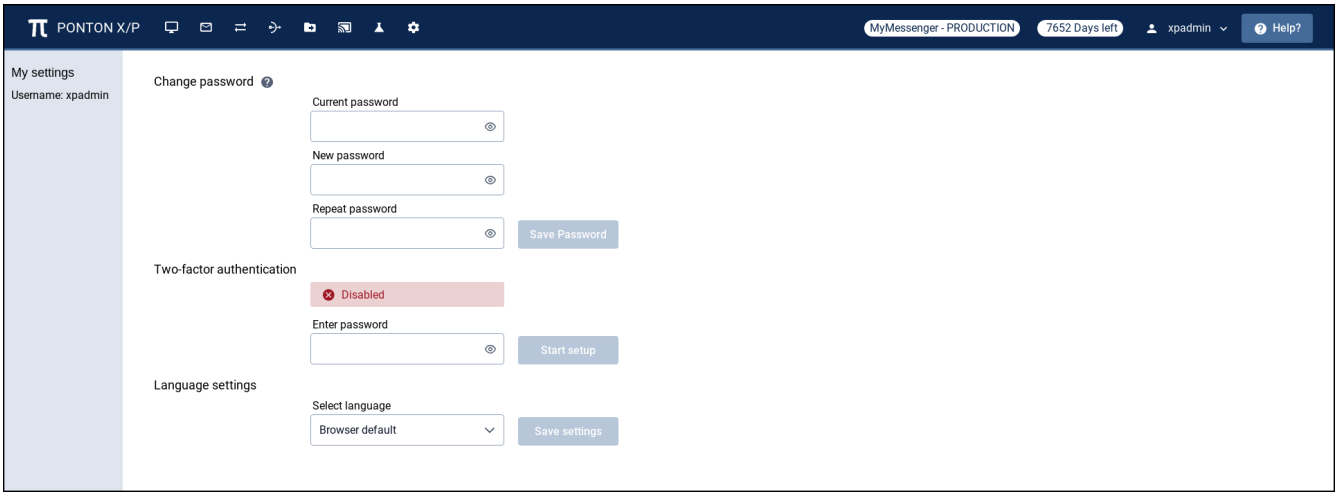
19. Two-Factor Authentication

You can configure two-factor authentication with time-based one-time passwords in the user settings.

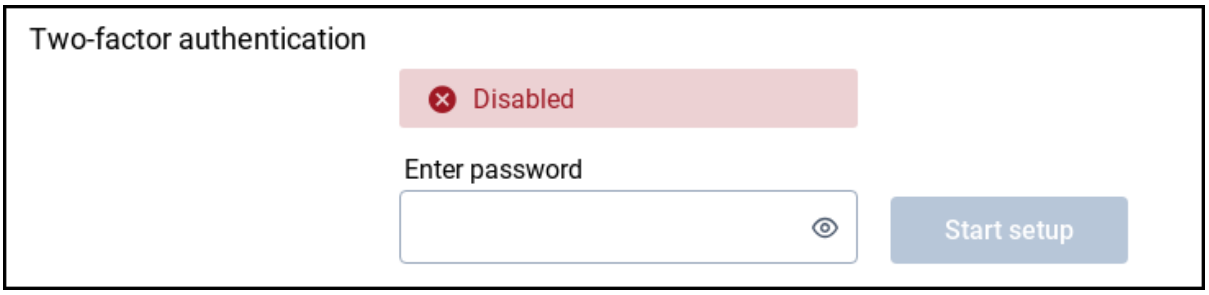
19.1. Prerequisites

To use two-factor authentication you will need an authenticator app (e.g. Microsoft Authenticator) that supports time-based one-time passwords.

19.2. Setup

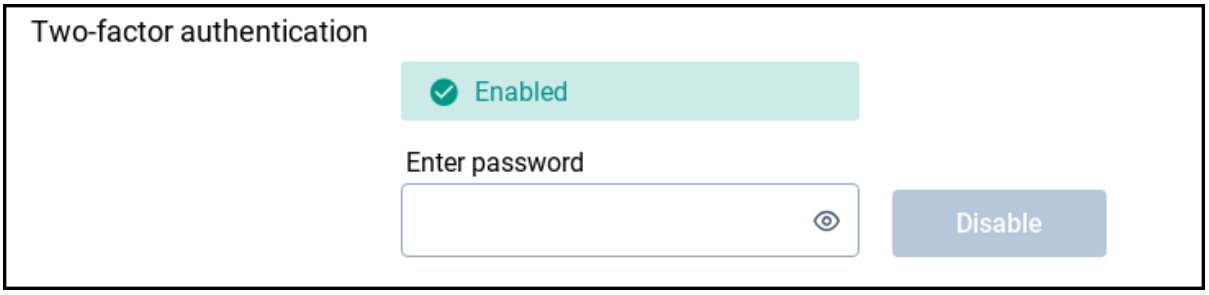


1. Start by entering your current password into the "Verify password" input and press "Start Setup"

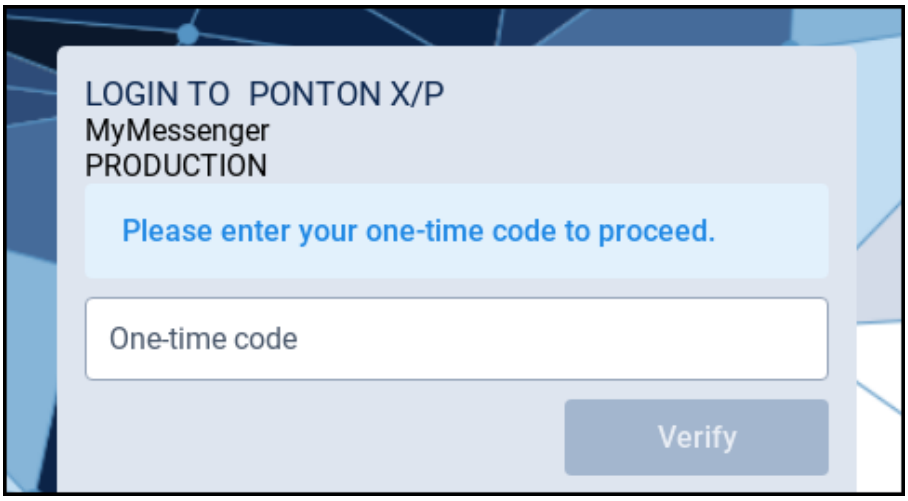


2. Now you should see a generated secret and a QR code. Scan that QR code with your authenticator app or alternatively copy the secret manually.

3. You authenticator app should now generate a six-digit code. Enter this code into the "Verify one-time code" input and press "Enable"

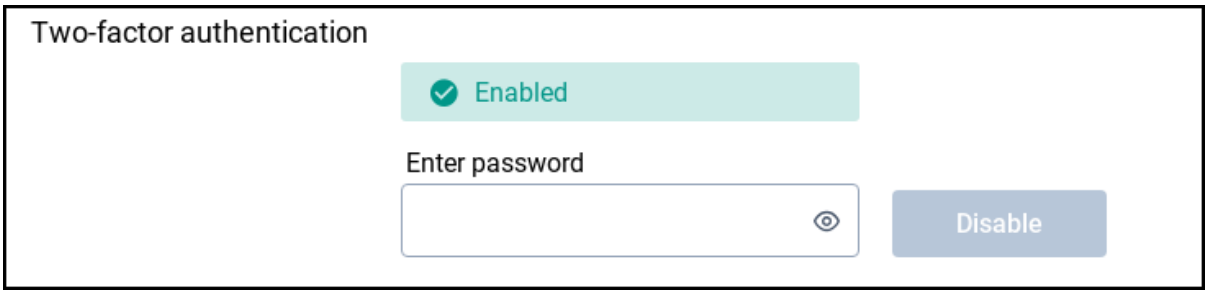


Now logging in with this user will prompt you for the six-digit one-time code from you authenticator app.



19.3. Disable

To disable two-factor authentication you will need to provide your current password to the "Verify password" input and press "Disable"



19.4. Change Secret / Reconfigure

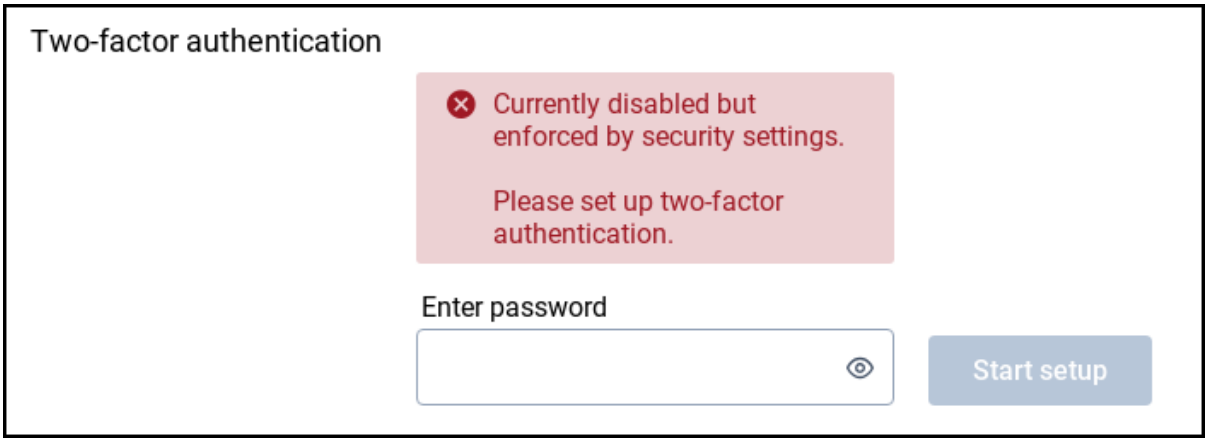
In order to reconfigure the secret just disable and re-enable two-factor authentication.

19.5. Enforce Two-Factor Authentication

You can require two-factor authentication for all users by going to "User Admin" > "Security Settings" and tick the "Enforce two factor authentication" checkbox before saving.

Note: This option cannot be disabled from the GUI/REST API. To disable it you will need to change Server/SecuritySettings/EnforceTwoFactors to false in the config/server.xml.

Once enforced all users without two-factor authentication will be redirected to the settings page, next time they log-in, to set it the two-factor authentication. The GUI functionality is locked until the two-factor authentication is configued.


Two-factor authentication
Currently disabled but enforced by security settings.
Please set up two-factor authentication.
Enter password
Start setup

20. REST API Documentation

The PONTON X/P Messenger is using Swagger UI to generate an interactive API documentation that enables you to try out the API calls directly in the browser. SwaggerUI is included in the X/P Messenger and also allows you to configure your X/P Messenger via the REST API.

20.1. Authentication

Most of the API endpoints require an authentication, which is indicated with a lock symbol in the Swagger UI.

There are two options for a REST API client to authenticate:

20.1.1. Json-Web-Token (JWT)

A JWT has to be acquired by sending a POST request to /api/authenticate endpoint with a HTTP body containing the user and password like this:

```
{
  "username": "<YOUR_USERNAME>",
  "password": "<YOUR_PASSWORD>"
}
```

The response will contain a JSON text containing a token like this:

```
{
  "username": "xpadmin",
  "token":
"eyJhbsciOiJIUzUxMiJ9.eyJTQUxUIjosMzFmOTljNzYtMDdiMy00M2EyLThhOTYtZTVhY1U0NDExZWI5Iiwi
cmVtb3RlSVAiOiIxMC45LjAuMzciLCJmb3J3YXJkZWRGb3IiOiIiLCJzdWIiOiJ4cGFkbWluIiwiaWF0IjoxNj
kyODE1NjUwLCJleHAiOjE2OTI4MzM2NTB9.FPMfobMoOki1sMBFSbK5kq4SEowfhve7qZu1E9cLVPcjNduzQoA
QOvGo3duM3sDNxgMhNp6fCCYcTEbCpsF4rQ"
}
```

The token value has to be included with any request that requires authentication. To do this, a HTTP header "Authorization" with value "Bearer eyJhbsciOiJIUzUxMiJ9.eyJTQUxUI....." has to be set.

The tokens are valid for a limited time, and a new token has to be requested if the authentication fails due to an expired token.

⚠️ When two-factor-authentication is required, then the authentication request must contain a valid TOTP code for the user as shown in this example:

```
{
  "username": "<YOUR_USERNAME>",
```

```
  "password": "<YOUR_PASSWORD>",
  "totp": "123456"
}
```

20.1.2. TLS Client Authentication

An alternative to Json-Web-Token is to set a TLS client certificate, when calling the API.

The used client certificate must be installed in the User Admin page.

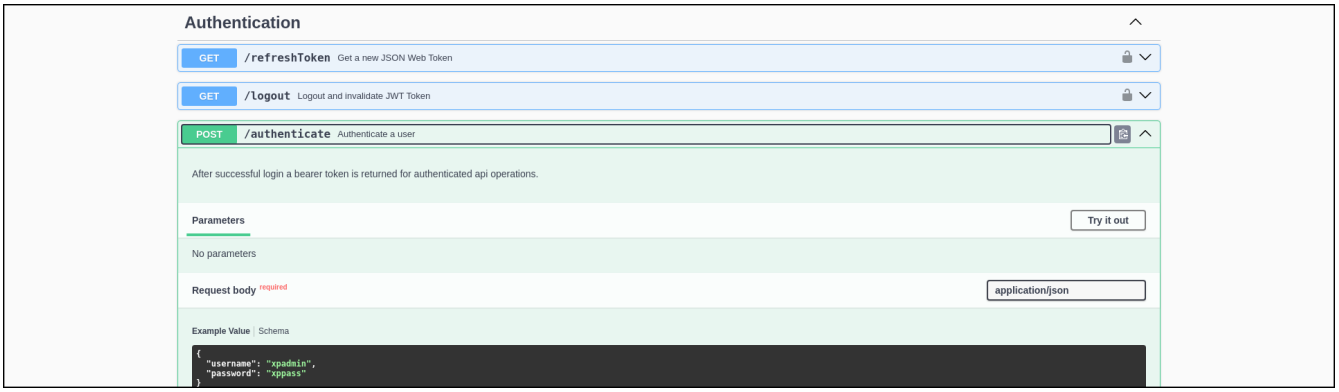
20.2. Using Swagger UI

You can find SwaggerUI at
http(s)://<YOUR_MESSENGER_HOST>:<YOUR_MESSENGER_PORT>*/api/swagger-ui*

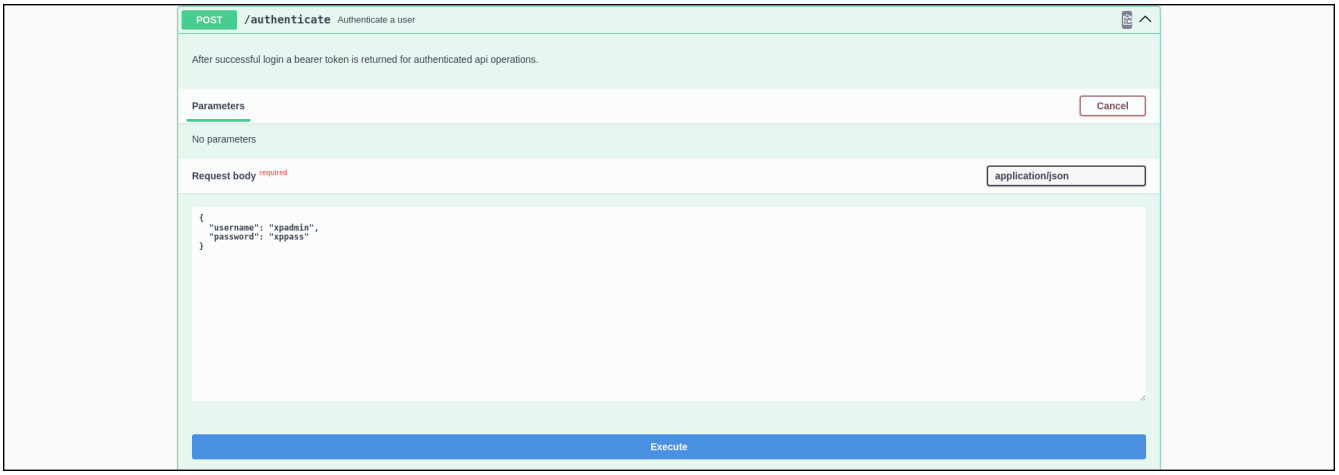
Make sure to replace <YOUR_MESSENGER_HOST> and <YOUR_MESSENGER_PORT> with your actual host and port.

Before any other request you need to send a POST Request to /authenticate to login. To do so open http(s)://<YOUR_MESSENGER_HOST>:<YOUR_MESSENGER_PORT>/api/swagger-ui/index.html?configUrl=/api/v3/api-docs/swagger-config#/Authentication/createAuthenticationToken in your browser

You should now see something like this:



Now click on "Try it out".



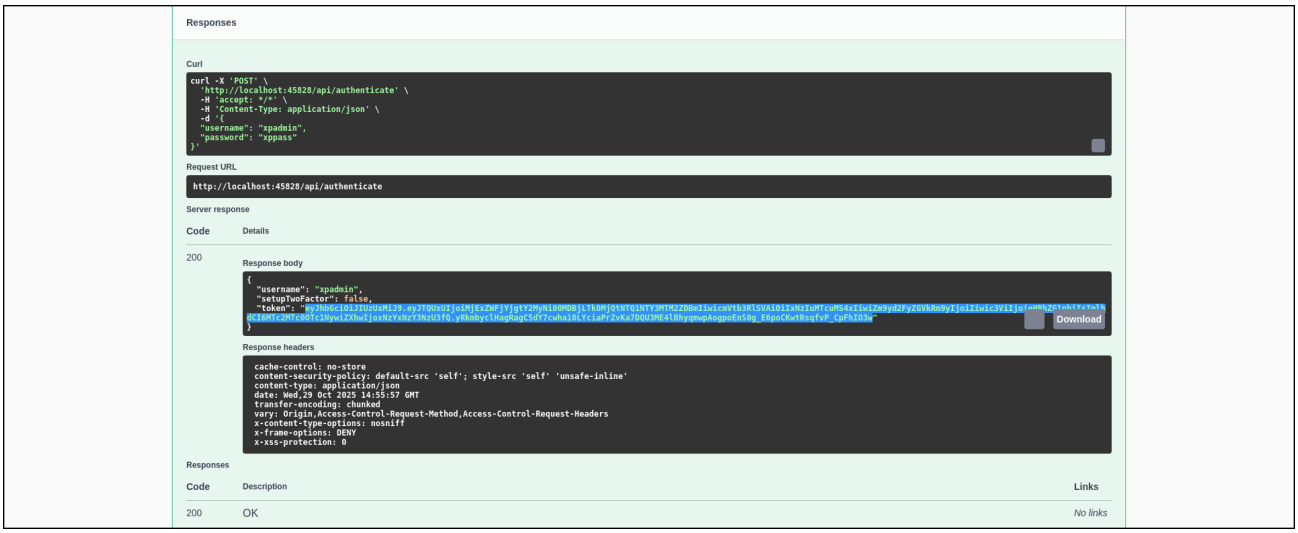
It should now show a text input prefilled with:

```
{
  "username": "xpadmin",
  "password": "xppass"
}
```

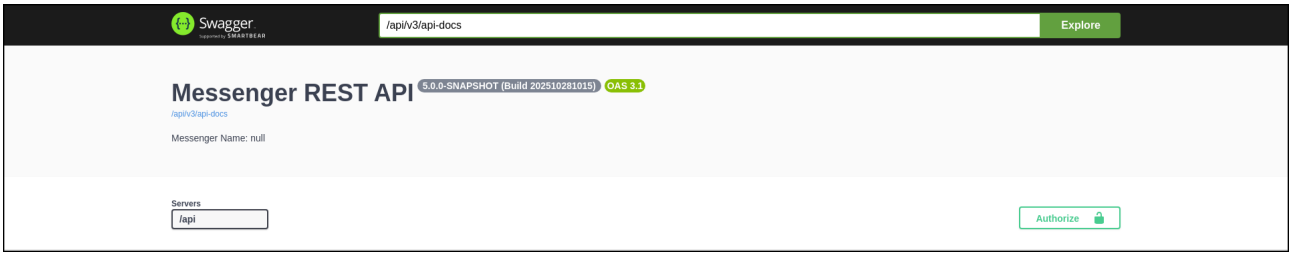
replace all of that with:

```
{
  "username": "<YOUR_USERNAME>",
  "password": "<YOUR_PASSWORD>"
}
```

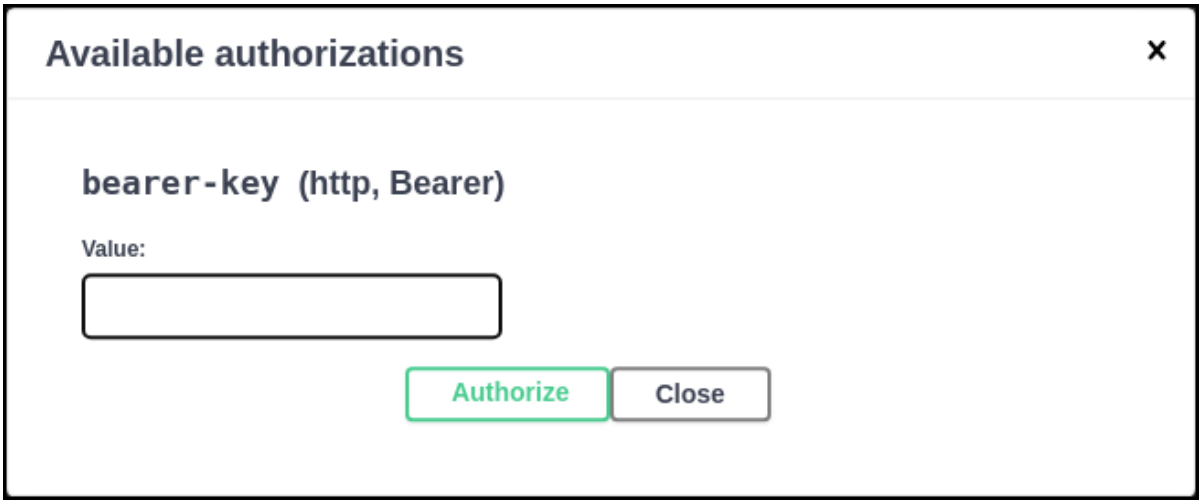
Now click on the blue "Execute" button at the bottom of the page.
If successful the server response below should look like this with a status code of 200:



Copy the text between the quotation marks after "token:" (selected in blue in the image).
Then click the "Authorize" button at the top.



Lastly paste the previously copied token into the dialog and submit by pressing the "Authorize" button in the dialog.

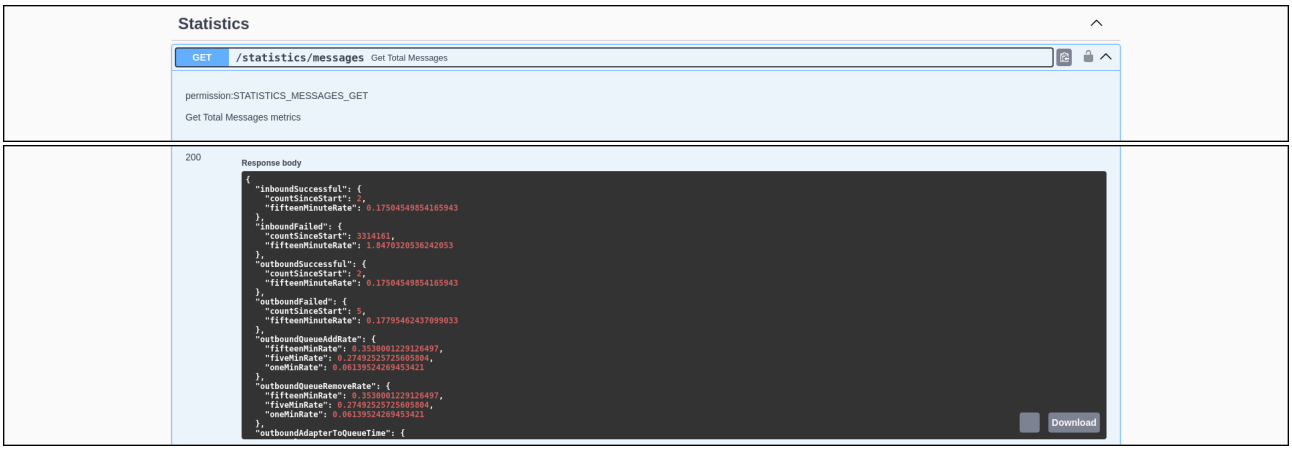


Now you should be able to perform any other operation.

20.3. Statistics

To find out how many messages were sent or received since the last Messenger start you have to call the following REST endpoint:
http(s)://<YOUR_MESSENGER_HOST>:<YOUR_MESSENGER_PORT>/**api/statistics/messages**

This can be done with the Swagger UI:



- inboundSuccessful
  - countSinceStart - number of successfully received messages since last restart
  - fifteenMinuteRate - average number of successfully received messages per second within the last 15 minutes
- inboundFailed
  - countSinceStart - number of failed inbound messages since last restart
  - fifteenMinuteRate - average number of failed inbound messages per second within the last 15 minutes
- outboundSuccessful
  - countSinceStart - number of successfully sent messages since last restart
  - fifteenMinuteRate - average number of successfully sent messages per second within the last

15 minutes

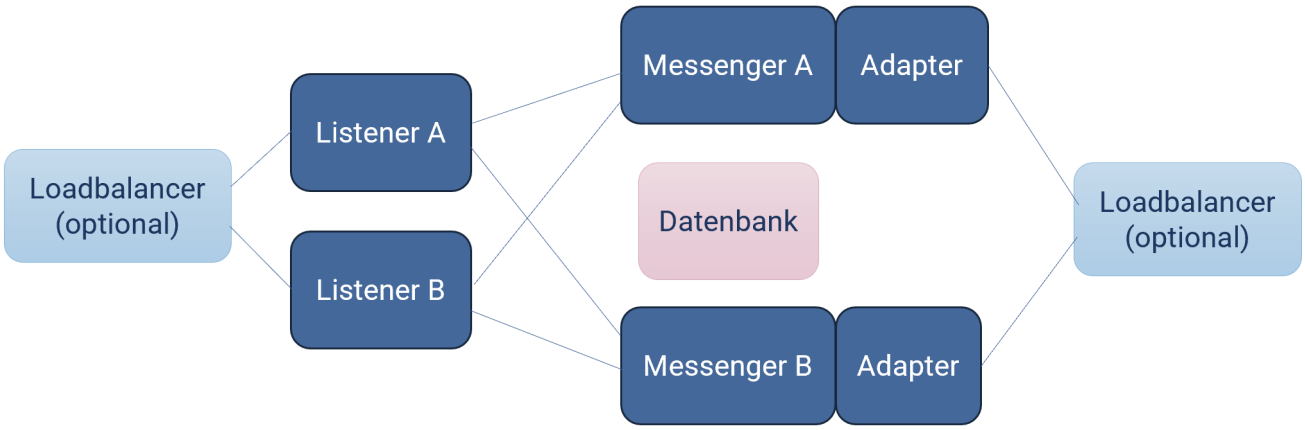
- outboundFailed
  - countSinceStart - number of failed outbound messages since last restart
  - fifteenMinuteRate - average number of failed outbound messages per second within the last 15 minutes
- outboundRetries - number of send retries since last restart
- outboundTransmissionTime - average message transmission time in seconds

It is possible to obtain similar statistical values for only one partner by calling the following REST endpoint:
http(s)://<YOUR_MESSENGER_HOST>:<YOUR_MESSENGER_PORT>/**api/statistics/messages/<PARNTER_ID>**

Be sure to replace <PARTNER_ID> with the partner id of need partner.

21. How to Setup a Cluster Using PONTON X/P Messengers and Listeners

To ensure high availability in case of planned or unplanned downtimes, **PONTON X/P** supports the setup of multiple Messenger and Listener nodes that work together as a unified cluster. This typically requires a **distributed environment** where each node operates on a separate machine.



21.1. Prerequisites for a Cluster Setup

Before setting up a cluster-based environment, ensure the following conditions are met:

21.1.1. Licensing

- Verify that your **PONTON X/P license** supports clustered Messenger usage.
- If you do not have such a license, please contact the **PONTON X/P Helpdesk**.

21.1.2. Essentially Shared Resources Across Nodes

The following shared resources are required to coordinate configuration and message data across nodes:

21.1.2.1. Database

- Provide a central **database** as outlined in **InstallationGuide#Database URL**.
- Ensure the database is **accessible by all PONTON X/P cluster nodes**.
- The PONTON X/P configuration, transmitted messages and other messaging related data will be stored in the same database schema and accessed by all nodes. Hence, all nodes have identical configurations.

21.1.3. Optionally Shared Resources Across Nodes

21.1.3.1. File System

Although each node has it's own local installation there can be cases where shared folders might be required across nodes for the following reasons:

21.1.3.1.1. Hotfolder Adapter

- To exchange payloads between backend systems and Messenger nodes Hotfolder Adapters can be used. If you wish to use the same Hotfolder Adapter across multiple nodes please ensure to set folder paths which are accessible by all nodes.

> **TIP** For hotfolder setup, refer to the chapter Hotfolder.

21.1.3.1.2. Http Adapter

- To exchange payloads between backend systems and Messenger nodes HTTP Adapters can be used. If you wish to use the same HTTP Adapter across multiple nodes please ensure to set folder path for incoming messages and Acknowledgements so that these folders are accessible by all nodes.

> **TIP** For HTTP Adapter setup, refer to the chapter Http Adapter.

21.1.3.1.3. Archive System

- Choose an appropriate **archiving solution** based on your requirements.
- The archive system must be **accessible by all cluster nodes**.
- See the Archiver Type section in Messenger >Settings for setup details.

21.2. Installation Procedure

21.2.1. Messenger Nodes in a Cluster

21.2.1.1. Step 1: Install the First Messenger Node

1. Unpack the Messenger on the target machine.
2. Set up your preferred **database** as described in InstallationGuide#Database Setup.
3. Start the Messenger node.
4. Complete the **Initial Setup** (refer to the respective chapters in the documentation).

21.2.1.2. Step 2: Install Additional Messenger Nodes

1. Unpack the Messenger on a new machine. Each node needs an individual Messenger installation.
2. Configure it to use the **same database** as the first node.

> **TIP** Since each node connects itself to the same database, it shares the same configuration as the other nodes. This implies that the required **ports etc. are open and available**

on all machines participating in the cluster.

NOTE	Provide the appropriate **database driver** as described in **InstallationGuide#Database Setup**.

3. Start the Messenger node.

NOTE	The new Messenger node will **automatically join the cluster** upon startup.

21.2.2. Listener Nodes in a Cluster (Optional)

21.2.2.1. Step 1: Install the First Listener Node

1. Unpack the Listener on the designated machine.
2. Complete the Listener setup (refer to documentation).
3. Start the Listener node.
4. Connect this Listener to the Messenger cluster.
5. Complete the listener configuration via Messenger UI. TIP: Refer to Enter Listener Connection settings in Messenger >Settings.

21.2.2.2. Step 2: Install Additional Listener Nodes

- Repeat steps **1.1** through **1.5** for each new Listener node. Each node needs an individual Listener installation.
- Multiple listeners can be connected to the same messenger cluster. Please refer to Enter Listener Connection settings in Messenger >Settings. In this case please ensure to install an SSL Certificate on the listener so that the CN is suitable for all the listeners in this cluster.

TIP	Since each node connects itself to the same database, it shares the same configuration as the other nodes. This implies that the required **ports etc. are open and available** on all machines participating in the cluster.

22. Appendix

22.1. AS4-BDEW at a glance

This document contains the specific requirements from the AS4-BDEW specification. It presumes, that you are familiar with the basic setup of the PONTON X/P Messenger.

22.1.1. Preparation

Before you start with configuring the Messenger Settings, the BDEW-Config patch must be installed.

22.1.2. BDEW Config Patch

1. Download AS4-BDEW-Config-Patch-XP460.zip: https://www.ponton.de/downloads/xp/bdew/AS4-BDEW-Config-Patch-XP460.zip
2. Unzip the AS4-BDEW-Config-Patch-XP460.zip in the /update Folder in your Messenger installation directory.
3. Re-start the Messenger
4. In the WebGUI of the Messenger you should see the following under „Installed Add-ons":

AS4-BDEW <current_version>

22.1.3. Messenger Settings

- **Message ID domain** must have a unique domain name such as domain.teilnehmer.de
- **Communication ⇒ SSL Server Certificate check**: Must be enabled, to ensure SSL Server Certificates are checked regularly for revocation by CA
- **Communication ⇒ Partner certificate revocation check:** Must be enabled, to ensure partner certificates and SSL Client Certificates are checked regularly for revocation by CA

All RootCA certificates should be installed under Messenger → Partners → My Partners → ✎ → Certificates → Install CA certificate:

- PONTON has stored all the certificates on our download server:
  - TEST: https://www.ponton.de/downloads/xp/bdew/sm-test-pki-de-CA.zip
  - PROD: https://www.ponton.de/downloads/xp/bdew/sm-pki-de-CA.zip

22.1.4. Partner Setup

To identify the partner properly a PartyID must be set. There are three **Party-ID-Types** available which must be used according to the AS4-BDEW profile specification:

- urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088
- urn:oasis:names:tc:ebcore:partyid-type:unregistered:BDEW

- urn:oasis:names:tc:ebcore:partyid-type:unregistered:DVGW

[Info Icon] Only one Party-ID is allowed for a remote or local partner profile, as defined in the AS4-BDEW profile.
[Info Icon] In case multiple codes exist, please verify which code to use for which purpose using the following link: https://bdew-codes.de/Codenumbers/BDEWCodes/CodeOverview

22.1.4.1. Automatic remote partner setup completion

Once a valid remote partner is created and saved an automatic download of remote partner certificates is performed by the messenger. The pre-requisites and results are identical to the 'Automatic partner certificate and URL updates'.

22.1.4.2. Partner Certificates

The KeyPair of the partner certificate must be of type EC **brainpoolP256r1**. You need to either install a certificate of this type which you have received from a trusted Certificate Authority (CA) or you create a certificate request of this type in the PONTON X/P Messenger (see Partner → Certificates + Request Certificates). Furthermore, you can also create requests for a certificate triple (TLS, SIGnatur and ENCryption) for AS4-BDEW which can be submitted to the Sub-CA of your choice.

22.1.4.3. Automatic remote partner certificate and URL updates

Remote partner certificates can be updated automatically by enabling the 'partner certificate revocation check' (see Messenger >Settings#Enter Communication settings).

Only partner profiles where no valid certificates are installed or profiles where the currently installed certificates are about to expire in less than 10 days are considered for updates.

[Info Icon] An important pre-requisite for the automatic check is that at least one of the local partners must contain a valid TLS certificate (as per BSI PKI_Certificate_Policy_v1.1.2).

The certificate check can only find suitable certificate matches from the respective **Sub-CAs** if a valid Party-ID Type is defined for the remote partner (see Partner Setup). If the check for certificate updates finds matching certificates (with CNs containing EMT.MAK) for the party-Id within the Sub-CAs storage, then they will automatically be stored into the remote partner profile.

The URLs contained in the downloaded TLS certificates, are automatically applied to the Remote Partner profiles.

Additionally, if the 'allow certificate update from received messages' is activated (see Messenger >Partner#Allow certificate update from received messages), the new partner certificates are automatically enhanced while processing incoming messages from these partners.

22.1.5. Agreement Setup

Agreements must be created with the new template AS4-BDEW after successfully setting up the partner profiles (including installation of AS4-BDEW certificates for those Local and Remote Partners).

[Info Icon] This will initialize all packaging fields with the required values for the AS4-BDEW-profile automatically:

Parameter	Value
Role (From)	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
Role (To)	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
Service	http://docs.oasis-open.org/ebxml-msg/as4/200902/service
Action	http://docs.oasis-open.org/ebxml-msg/as4/200902/action
Agreement reference (type and pmode must be empty)	https://www.bdew.de/as4/communication/agreement
Sign messages	SHA256 / ECDSA / BINARY_SECURITY_TOKEN_PKIPATH **The latest SIG Certificate from the local partner profile is selected automatically.**
Expect signed messages	AES128_GCM / ECDH-ES-ConcatKDF-empty-sha256 / SUBJECT_KEY_IDENTIFIER
Encrypt messages	AES128_GCM / ECDH-ES-ConcatKDF-empty-sha256 / SUBJECT_KEY_IDENTIFIER **The latest ENC Certificate from the remote partner profile is selected automatically.**
Expect encrypt messages	AES128_GCM
Send receipts	Send signed receipts: SHA256 / ECDSA / BINARY_SECURITY_TOKEN_PKIPATH **The latest SIG Certificate from the local partner profile is selected automatically.**
Expect receipts	Expect signed receipts: SHA256 / ECDSA

22.1.5.1. Automatic certificate pre-selections and switch

As soon as new partner certificates are updated in the Local or Remote Partner profiles the respective AS4 BDEW agreements with these partners will also be updated automatically with pre-selected ENC and/or SIG certificates. This pre-selection is done based on the key usage and validity period of the certificates available. As soon as (SIG or ENC) certificates with a longer validity period (more than 30 days) are installed in the partner profiles, the respective SIG / ENC certificates in the agreements are switched automatically.

22.1.6. Schema Set for Path Switch

There is a schema set "AS4-BDEW-PathSwitch" which must be activated for Partners and Agreements. This enables message of PathSwitch type, which is used for switching the communication to the AS4-BDEW profile. The back-end of the user should be able to process the two message types "Request Switch" and "Confirm Switch".

22.1.7. Listener Configuration

Check the following settings:

- Under Listener → Settings
  Deactivate **Client certificate check (Identity)**. This check only allows messages to be sent using certificates that are installed in the Listener.
- Under Listener → Client certificates
  All RootCA certificates should be installed here.
  PONTON has stored all the certificates on our download server:
  - TEST: https://www.ponton.de/downloads/xp/bdew/sm-test-pki-de-CA.zip
  - PROD: https://www.ponton.de/downloads/xp/bdew/sm-pki-de-CA.zip

22.1.8. TLS certificates

22.1.8.1. Listener certificate (of local partners)

The TLS certificates of Local Partners (see Messenger >Partner#Partner Certificates) can be installed on the Listener (see Listener Configuration and Certificates#Install Listener Certificate) manually. In case you have assigned different URLs to different Local Partners in your Messenger and you are using the Listener for inbound communication, then you are required to install the TLS certificates of all the required Local Partners on the Listener individually.

[Info Icon] Although a valid TLS certificate (as per BSI PKI_Certificate_Policy_v1.1.2) can be installed on the Messenger (see Messenger >Settings#Server certificate) , this is currently not supported for incoming TLS communication. A TLS certificate installed on the Messenger server leads to connection errors.

22.1.8.2. CA certificates (of Sub-CAs)

These certificates of Sub-CAs are retrieved and updated automatically at regular intervals, as long as the root CA certificates are already installed on the listener and messenger.

[Info Icon] This requires at least one Local Partner which has a valid TLS certificate, issued by a Sub-CA, installed in its profile. This will allow the Messenger to establish a secure connection to RootCA's LDAP server, where the corresponding certificates of Sub-CAs are published. The Messenger will download and install these certificates automatically at startup and will check for updates every 24h. The retrieved Sub-CA certificates are installed into the Listener, automatically, if checkbox "Use partner certificates" is enabled in the Listener's configuration.

[Info Icon] These CA certificates of the Sub-CAs are also installed into the Messenger automatically.

22.1.9. Hints

22.1.9.1. Firewall Rules

22.1.9.1.1. Inbound

It is required that the external access to the Listener is not restricted.

22.1.9.1.2. Outbound

The Messenger needs to be able to reach all Sub-CAs on port 636 and 389 either directly or using a HTTP Proxy (see **external server links for certificates**). The Messenger needs to be able to reach the URLs of the market participants either directly or using a HTTP Proxy.

22.1.9.2. Test & Production relevant PKI, Root-CA and Sub-CA values

As described under Messenger >Settings#Display it is possible to define the Messenger instance as TEST or PRODUCTION system. This selection has a direct effect on the endpoint values used for the respective purposes :

Purpose	Test value	Production value
Relevant for certificate triple requests	SM-Test-PKI-DE	SM-PKI-DE

Purpose	Test value	Production value
Relevant for downloading and revocation of AS4 market participant certificates	From the listed test Sub-CAs the following test Sub-CAs are **actively supported** currently: • T-Systems-EnergyCA (ldaps://ldap.energyca.test.telesec.de) • CA4Energy-EKN-Test.CA (ldaps://ldap.energyca.test.telesec.de) • COUNT-CARE.CA (ldaps://ldap.cc-gwa-test.de) • SAG-Metering-Test.CA (ldaps://smgw-ldap-test.schleupen.de) • SM-Test-SmartService.CA (ldaps://ldap.smartserviceca.test.sm-pki.smartservice.de) • DARZ (ldaps://ldap.sm-test-pki-de.da-rz.net) • EVIDEN (ldaps://ldap.sm-pkitest.trustcenter-services.com) And the following server URLs are currently redundant and hence, not activated additionally: • ATOS / GWAdriga (ldaps://ldap.sm-pkitest.atos.net)	From the listed prod Sub-CAs the following Sub-CA is actively supported currently: • CA4Energy-EKN.CA (ldaps://ldap.ekn-energyca.telesec.de) • COUNT-CARE.CA (ldaps://ldap.cc-gwa.de) • T-Systems-EnergyCA (ldaps://ldap.energyca.telesec.de) • DARZ (ldaps://ldap.sub-ca.da-rz.net) • EVIDEN (ldaps://ldap.sm-pki.trustcenter-services.com) • SmartService.CA (ldaps://ldaps.smartserviceca.sm-pki.smartservice.de) • Schleupen-Smart-Metering-Sub.CA (ldaps://ldap.smpki.schleupen.cloud) And the following server URLs are currently redundant and hence, not activated additionally: • ATOS (ldaps://ldap.sm-pki.atos.net) • GWAdriga-SmartEnergy.CA (ldaps://ldap.gwadriga.de)
Relevant for certificate triple requests (for certificate updates)	Actively supported webservices: DARZ.CA (https://test.sub-ca.da-rz.net:8443/metering-ca/services/SmartMeterService), T-Systems-EnergyCA (https://energyca.test.telesec.de/energycatest/131/services/SmartMeterService) and SmartService.CA (https://ws.smartserviceca.test.sm-pki.smartservice.de:443/api/smartmeter)	

Purpose	Test value	Production value
Relevant for retrieving CA certificates of (**actively supported**) Sub-CAs and install them on the messenger and listener	ldaps://ldap.root.test.sm-pki.telesec.de	ldaps://ldap.root.sm-pki.telesec.de

22.1.10. Sending XML files with EIC codes, although market communication requires BDEW codes

Since EIC codes are used (for FPM "Fahrplanmanagement") instead of BDEW codes when sending load schedules to the TSOs, one of the following setups is required to enable successful partner recognition as well as successful AS4 compliant market communication:

1. Activate the option ‘Use partner subfolder’ in the Hotfolder Adapter (see Hotfolder#Enter Outbox Settings). Subfolders are then automatically created for all existing communication partners with the respective backend partner ID. All files that are then stored in the respective partner folder are sent to the corresponding partner regardless of the codes within the file.
2. Alternatively, the files could be sent via the HTTP adapter. There, the recipient can be explicitly transmitted as a parameter such X-BackendSenderId or X-BackendReceiverId (see Http Adapter#Outbound Direction).

22.2. Database structure

The Messenger uses a database to store configuration, message data as well as meta information about all sent and received messages.
It is possible to query these tables by external applications, but this is no official interface to the application and there might be changes when the Messenger is upgraded.

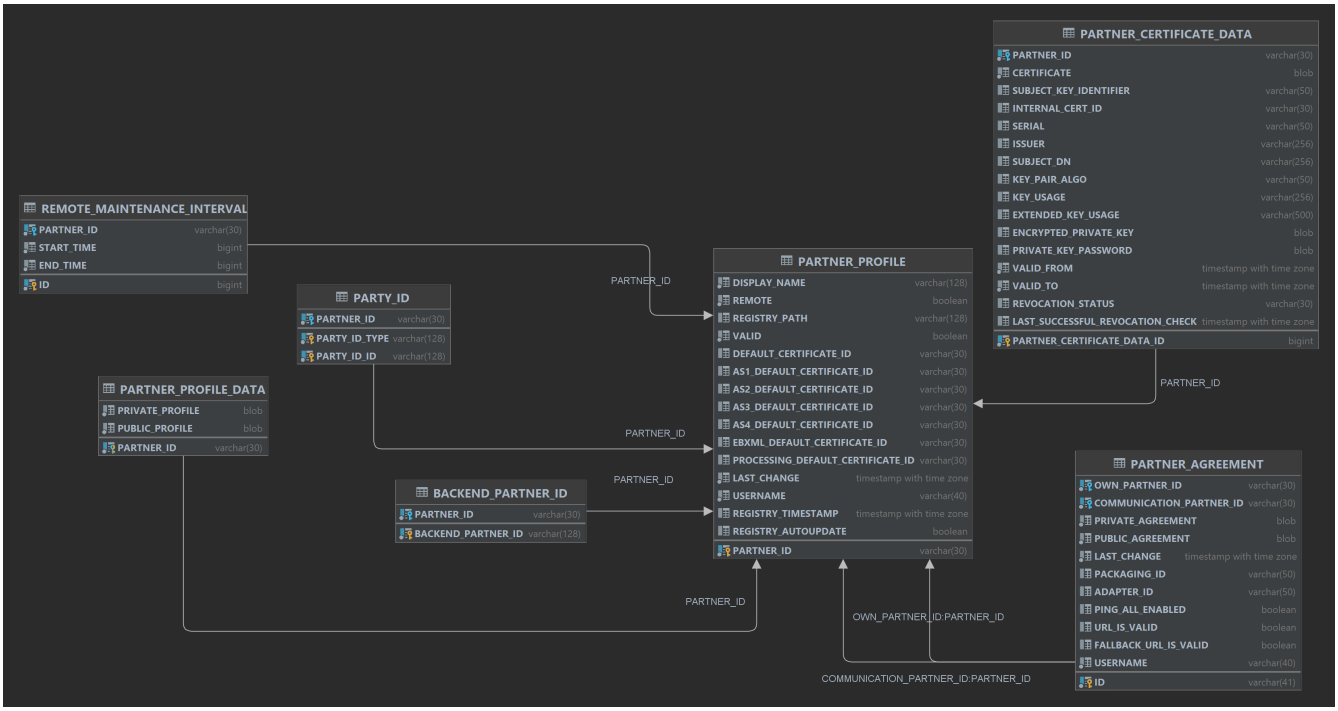
Therefore, any direct database access is not recommended and on your own risk.

22.2.1. Overview

This section provides a summary of the database schema of the PONTON X/P messenger. It could help understand what each area of the database represents and shows how they relate to each other based on their technical constraints.

22.2.1.1. Partner Management

This section represents database entities that are related to partners which are required for message exchange through the system.



22.2.1.1.1. partner_profile

Describes each partner’s identity and configuration.

Column	Type
PARTNER_ID	VARCHAR(30)
DISPLAY_NAME	VARCHAR(128)
REMOTE	BOOLEAN
REGISTRY_PATH	VARCHAR(128)

VALID	BOOLEAN
DEFAULT_CERTIFICATE_ID	VARCHAR(30)
AS1_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
AS2_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
AS3_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
AS4_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
EBXML_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
PROCESSING_DEFAULT_CERTIFICATE_ID	VARCHAR(30)
LAST_CHANGE	TIMESTAMP WITH TIME ZONE
USERNAME	VARCHAR(40)
REGISTRY_TIMESTAMP	TIMESTAMP WITH TIME ZONE
REGISTRY_AUTOUPDATE	BOOLEAN

Keys:

- PK_PARTNER_PROFILE → (PARTNER_ID)

Foreign Keys: - None

22.2.1.1.2. partner_profile_data

Contains each partner's public and private profile data in binary form.

Column	Type
PARTNER_ID	VARCHAR(30)
PRIVATE_PROFILE	BLOB
PUBLIC_PROFILE	BLOB

Keys:

- PK_PARTNER_PROFILE_DATA → (PARTNER_ID)

Foreign Keys:

- FK_PARTNER_PROFILE_DATA_PARTNER_ID → PARTNER_PROFILE(PARTNER_ID)

22.2.1.1.3. partner_certificate_data

Stores certificate information of each partner.

Column	Type
PARTNER_CERTIFICATE_DATA_ID	BIGINT
PARTNER_ID	VARCHAR(30)

CERTIFICATE	BLOB
SUBJECT_KEY_IDENTIFIER	VARCHAR(50)
INTERNAL_CERT_ID	VARCHAR(30)
SERIAL	VARCHAR(50)
ISSUER	VARCHAR(256)
SUBJECT_DN	VARCHAR(256)
KEY_PAIR_ALGO	VARCHAR(50)
KEY_USAGE	VARCHAR(256)
EXTENDED_KEY_USAGE	VARCHAR(500)
ENCRYPTED_PRIVATE_KEY	BLOB
PRIVATE_KEY_PASSWORD	BLOB
VALID_FROM	TIMESTAMP WITH TIME ZONE
VALID_TO	TIMESTAMP WITH TIME ZONE
REVOCATION_STATUS	VARCHAR(30)
LAST_SUCCESSFUL_REVOCATION_CHECK	TIMESTAMP WITH TIME ZONE

Keys:

- PK_PARTNER_CERTIFICATE_DATA → (PARTNER_CERTIFICATE_DATA_ID)

Foreign Keys:

- FK_PARTNER_CERTIFICATE_PARTNER_ID → PARTNER_PROFILE(PARTNER_ID)

22.2.1.1.4. partner_agreement

Defines communication agreements between two partners.

Column	Type
ID	VARCHAR(41)
OWN_PARTNER_ID	VARCHAR(30)
COMMUNICATION_PARTNER_ID	VARCHAR(30)
PRIVATE_AGREEMENT	BLOB
PUBLIC_AGREEMENT	BLOB
LAST_CHANGE	TIMESTAMP WITH TIME ZONE
PACKAGING_ID	VARCHAR(50)
ADAPTER_ID	VARCHAR(50)
PING_ALL_ENABLED	BOOLEAN
URL_IS_VALID	BOOLEAN

FALLBACK_URL_IS_VALID	BOOLEAN
USERNAME	VARCHAR(40)

Keys:

- PK_PARTNER_AGREEMENT → (ID)
- UQ_AGREEMENT → (OWN_PARTNER_ID, COMMUNICATION_PARTNER_ID)

Foreign Keys:

- FK_PARTNER_AGREEMENT_OWN_PROFILE → PARTNER_PROFILE(PARTNER_ID)
- FK_PARTNER_AGREEMENT_COMM_PROFILE → PARTNER_PROFILE(PARTNER_ID)

22.2.1.1.5. backend_partner_id

Maps internal partner IDs to external or backend system identifiers.

Column	Type
PARTNER_ID	VARCHAR(30)
BACKEND_PARTNER_ID	VARCHAR(128)

Keys:

- PK_BACKEND_PARTNER_ID → (BACKEND_PARTNER_ID)

Foreign Keys:

- FK_BACKEND_PARTNER_ID_PARTNER_ID → PARTNER_PROFILE(PARTNER_ID)

22.2.1.1.6. party_id

Stores external identifiers for partners.

Column	Type
PARTNER_ID	VARCHAR(30)
PARTY_ID_TYPE	VARCHAR(128)
PARTY_ID_ID	VARCHAR(128)

Keys:

- PK_PARTY_ID → (PARTY_ID_TYPE, PARTY_ID_ID)

Foreign Keys:

- FK_PARTY_ID_PARTNER_ID → PARTNER_PROFILE(PARTNER_ID)

22.2.1.1.7. remote_maintenance_interval

Defines maintenance time windows per partner.

Column	Type
ID	BIGINT
PARTNER_ID	VARCHAR(30)
START_TIME	BIGINT
END_TIME	BIGINT

Keys:

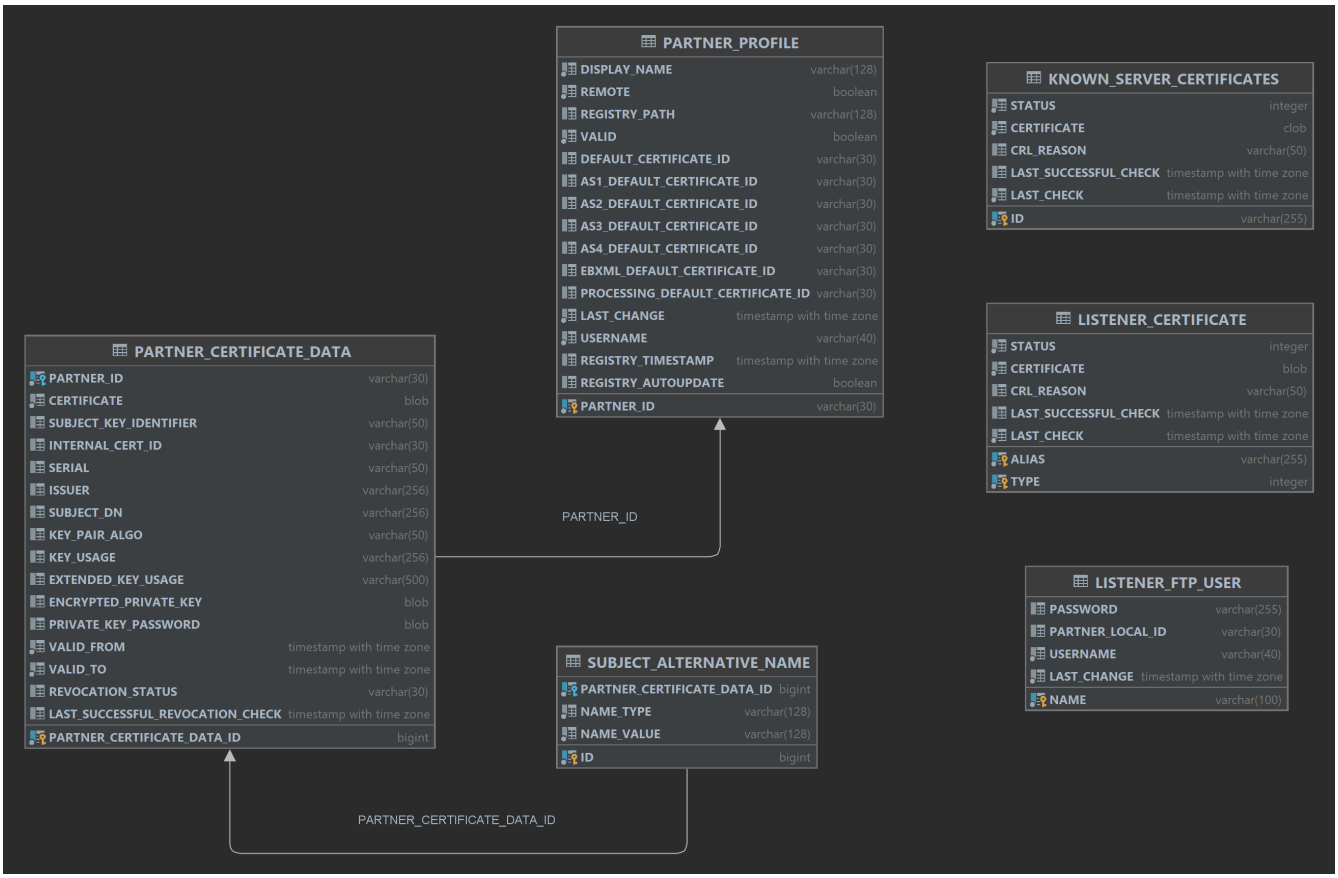
- PK_REMOTE_MAINTENANCE_INTERVAL → (ID)

Foreign Keys:

- FK_REMOTE_MAINTENANCE_INTERVAL_PARTNER_ID → PARTNER_PROFILE(PARTNER_ID)

22.2.1.2. Server Certificates

Manages keys, certificates, and trust relationships used to secure communication from messengers to listeners and vice versa.



22.2.1.2.1. subject_alternative_name

Holds the Subject Alternative Names (SAN) values for a certificate.

Column	Type
ID	BIGINT
PARTNER_CERTIFICATE_DATA_ID	BIGINT
NAME_TYPE	VARCHAR(128)
NAME_VALUE	VARCHAR(128)

Keys:

- PK_SUBJECT_ALTERNATIVE_NAME → (ID)

Foreign Keys:

- FK_SUBJECT_ALTERNATIVE_NAME_PARTNER_CERTIFICATE → PARTNER_CERTIFICATE_DATA(PARTNER_CERTIFICATE_DATA_ID)

22.2.1.2.2. listener_certificate

Stores listener-side certificates used for inbound connections.

Column	Type
ALIAS	VARCHAR(255)
TYPE	INTEGER
STATUS	INTEGER
CERTIFICATE	BLOB
CRL_REASON	VARCHAR(50)
LAST_SUCCESSFUL_CHECK	TIMESTAMP WITH TIME ZONE
LAST_CHECK	TIMESTAMP WITH TIME ZONE

Keys:

- P_LISTENER_CERTIFICATE → (ALIAS, TYPE)

Foreign Keys: - None

22.2.1.2.3. known_server_certificates

Holds server certificates and their respective status for outbound communication.

Column	Type
ID	VARCHAR(255)
STATUS	INTEGER
CERTIFICATE	CLOB
CRL_REASON	VARCHAR(50)
LAST_SUCCESSFUL_CHECK	TIMESTAMP WITH TIME ZONE
LAST_CHECK	TIMESTAMP WITH TIME ZONE

Keys:

- PK_KNOWN_SERVER_CERTIFICATES → (ID)

Foreign Keys: - None

22.2.1.2.4. listener_ftp_user

Defines user credentials and access settings for FTP-based listener interfaces.

Column	Type
NAME	VARCHAR(100)
PASSWORD	VARCHAR(255)
PARTNER_LOCAL_ID	VARCHAR(30)
USERNAME	VARCHAR(40)

LAST_CHANGE	TIMESTAMP WITH TIME ZONE

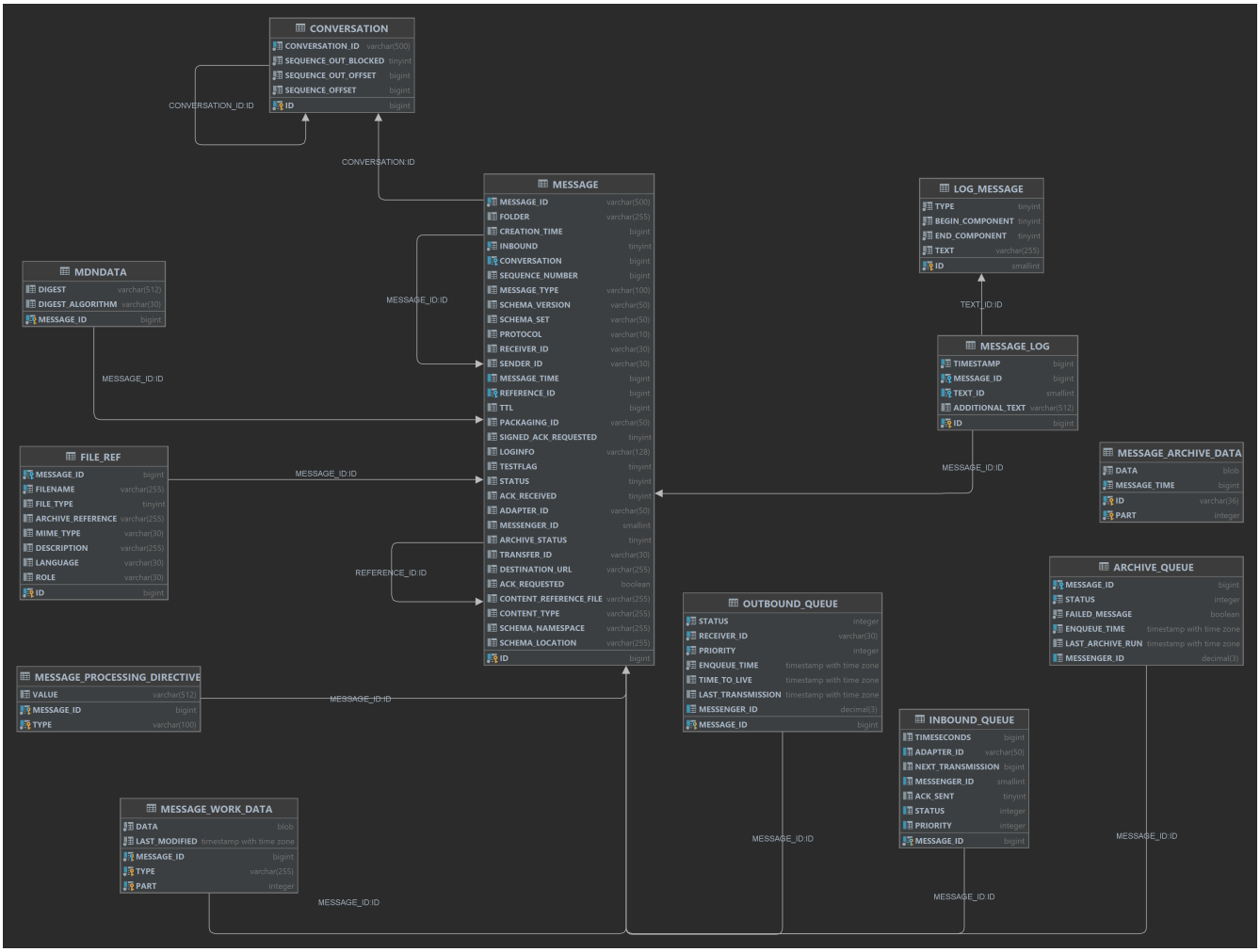
Keys:

- PK_LISTENER_FTP_USER → (NAME)

Foreign Keys: - None

22.2.1.3. Messaging Core

Stores and manages messages exchanged between partners.



22.2.1.3.1. message

Represents the main message entity.

Column	Type
ID	BIGINT
MESSAGE_ID	VARCHAR(500)
FOLDER	VARCHAR(255)
CREATION_TIME	BIGINT
INBOUND	TINYINT
CONVERSATION	BIGINT
SEQUENCE_NUMBER	BIGINT
MESSAGE_TYPE	VARCHAR(100)
SCHEMA_VERSION	VARCHAR(50)
SCHEMA_SET	VARCHAR(50)

PROTOCOL	VARCHAR(10)
RECEIVER_ID	VARCHAR(30)
SENDER_ID	VARCHAR(30)
MESSAGE_TIME	BIGINT
REFERENCE_ID	BIGINT
TTL	BIGINT
PACKAGING_ID	VARCHAR(50)
SIGNED_ACK_REQUESTED	TINYINT
LOGINFO	VARCHAR(128)
TESTFLAG	TINYINT
STATUS	TINYINT
ACK_RECEIVED	TINYINT
ADAPTER_ID	VARCHAR(50)
MESSENGER_ID	SMALLINT
ARCHIVE_STATUS	TINYINT
TRANSFER_ID	VARCHAR(30)
DESTINATION_URL	VARCHAR(255)
ACK_REQUESTED	BOOLEAN
CONTENT_REFERENCE_FILE	VARCHAR(255)
CONTENT_TYPE	VARCHAR(255)
SCHEMA_NAMESPACE	VARCHAR(255)
SCHEMA_LOCATION	VARCHAR(255)

Keys:

- PK_MESSAGE → (ID)
- UQ_MESSAGE → (MESSAGE_ID, INBOUND)

Foreign Keys:

- FK_MESSAGE_CONVERSATION → CONVERSATION(ID)
- FK_MESSAGE_MESSAGE → MESSAGE(ID)

22.2.1.3.2. conversation

Groups related messages into conversations, tracking sequence numbers.

Column	Type
ID	BIGINT

CONVERSATION_ID	VARCHAR(500)
SEQUENCE_OUT_BLOCKED	TINYINT
SEQUENCE_OUT_OFFSET	BIGINT
SEQUENCE_OFFSET	BIGINT

Keys:

- PK_CONVERSATION → (ID)
- UQ_CONVERSATION → (CONVERSATION_ID)

Foreign Keys: - None directly; referenced by MESSAGE(CONVERSATION)

22.2.1.3.3. file_ref

Associates attached files with messages.

Column	Type
ID	BIGINT
MESSAGE_ID	BIGINT
FILENAME	VARCHAR(255)
FILE_TYPE	TINYINT
ARCHIVE_REFERENCE	VARCHAR(255)
MIME_TYPE	VARCHAR(30)
DESCRIPTION	VARCHAR(255)
LANGUAGE	VARCHAR(30)
ROLE	VARCHAR(30)

Keys:

- PK_FILE_REF → (ID)
- UQ_FILE_REF → (MESSAGE_ID, FILENAME)

Foreign Keys:

- FK_FILE_REF_MESSAGE → MESSAGE(ID)

22.2.1.3.4. message_log

Stores per-message event entries and processing details.

Column	Type
ID	BIGINT
TIMESTAMP	BIGINT

MESSAGE_ID	BIGINT
TEXT_ID	SMALLINT
ADDITIONAL_TEXT	VARCHAR(512)

Keys:

- PK_MESSAGE_LOG → (ID)

Foreign Keys:

- FK_MESSAGE_LOG_MESSAGE → MESSAGE(ID)
- FK_MESSAGE_LOG_LOG_MESSAGE → LOG_MESSAGE(ID)

22.2.1.3.5. message_processing_directive

Defines additional metadata per message.

Columns	Type
MESSAGE_ID	BIGINT
TYPE	VARCHAR(100)
VALUE	VARCHAR(512)

Keys:

- PK_MESSAGE_PROCESSING_DIRECTIVE → (MESSAGE_ID, TYPE)

Foreign Keys:

- FK_MESSAGE_PROC_DIRECTIVE_MESSAGE → MESSAGE(ID)

22.2.1.3.6. message_work_data

Stores message content used during processing.

Columns	Type
MESSAGE_ID	BIGINT
TYPE	VARCHAR(255)
DATA	BLOB
PART	INTEGER
LAST_MODIFIED	TIMESTAMP WITH TIME ZONE

Keys:

- PK_MESSAGE_WORK_DATA → (MESSAGE_ID, TYPE, PART)

Foreign Keys:

- FK_MESSAGE_WORK_DATA_MESSAGE → MESSAGE(ID)

22.2.1.3.7. message_archive_data

Stores archived message data, split into parts if necessary.

Columns	Type
ID	VARCHAR(36)
PART	INTEGER
DATA	BLOB
MESSAGE_TIME	BIGINT

Keys:

- PK_MESSAGE_ARCHIVE_DATA → (ID, PART)

Foreign Keys: - None

22.2.1.3.8. mdndata

Stores hash values (digests) related to messages.

Columns	Type
MESSAGE_ID	BIGINT
DIGEST	VARCHAR(512)
DIGEST_ALGORITHM	VARCHAR(30)

Keys:

- PK_MDNDATA → (MESSAGE_ID)

Foreign Keys:

- FK_MDNDATA_MESSAGE → MESSAGE(ID)

22.2.1.3.9. inbound_queue

Contains inbound messages received from external partners and awaiting processing.

Column	Type
MESSAGE_ID	BIGINT
TIMESECONDS	BIGINT
ADAPTER_ID	VARCHAR(50)
NEXT_TRANSMISSION	BIGINT
MESSENGER_ID	SMALLINT

ACK_SENT	TINYINT
STATUS	INTEGER
PRIORITY	INTEGER

Keys:

- PK_INBOUND_QUEUE → (MESSAGE_ID)

Foreign Keys:

- FK_INBOUND_QUEUE_MESSAGE → MESSAGE(ID)

22.2.1.3.10. outbound_queue

Contains messages received from an adapter and ready to be sent to partners.

Column	Type
MESSAGE_ID	BIGINT
STATUS	INTEGER
RECEIVER_ID	VARCHAR(30)
PRIORITY	INTEGER
ENQUEUE_TIME	TIMESTAMP WITH TIME ZONE
TIME_TO_LIVE	TIMESTAMP WITH TIME ZONE
LAST_TRANSMISSION	TIMESTAMP WITH TIME ZONE
MESSENGER_ID	DECIMAL(3)

Keys:

- PK_OUTBOUND_QUEUE → (MESSAGE_ID)

Foreign Keys:

- FK_OUTBOUND_QUEUE_MESSAGE → MESSAGE(ID)

22.2.1.3.11. archive_queue

Holds messages ready for archiving.

Column	Type
MESSAGE_ID	BIGINT
STATUS	INTEGER
FAILED_MESSAGE	BOOLEAN
ENQUEUE_TIME	TIMESTAMP WITH TIME ZONE
LAST_ARCHIVE_RUN	TIMESTAMP WITH TIME ZONE

MESSENGER_ID	DECIMAL(3)

Keys:

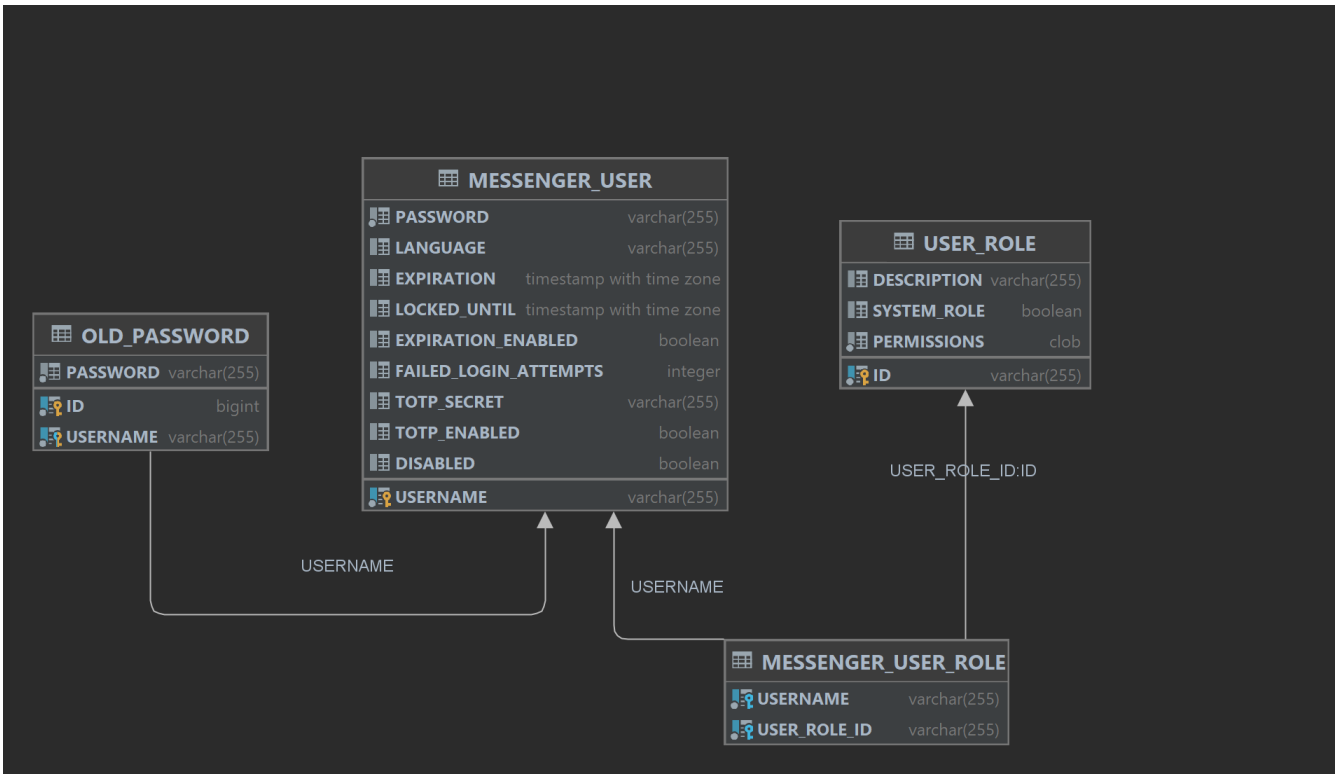
- AK_ARCHIVE_QUEUE → (MESSAGE_ID)

Foreign Keys:

- FK_MESSAGE_ARCHIVE_QUEUE_MESSAGE → MESSAGE(ID)

22.2.1.4. User and Role Management

Stores user account information, authentication data, and access-related preferences for messenger users.



22.2.1.4.1. messenger_user

Identification, login information and status of each user.

Column	Type
USERNAME	VARCHAR(255)
PASSWORD	VARCHAR(255)
LANGUAGE	VARCHAR(255)
EXPIRATION	TIMESTAMP WITH TIME ZONE
LOCKED_UNTIL	TIMESTAMP WITH TIME ZONE
EXPIRATION_ENABLED	BOOLEAN
FAILED_LOGIN_ATTEMPTS	INTEGER
TOTP_SECRET	VARCHAR(255)
TOTP_ENABLED	BOOLEAN
DISABLED	BOOLEAN

Keys:

- PK_MESSENGER_USER → (USERNAME)

Foreign Keys: - None

22.2.1.4.2. user_role

Defines user roles and permissions.

Column	Type
ID	VARCHAR(255)
DESCRIPTION	VARCHAR(255)
SYSTEM_ROLE	BOOLEAN
PERMISSIONS	CLOB

Keys:

- PK_USER_ROLE → (ID)

Foreign Keys: - None

22.2.1.4.3. messenger_user_role

Junction table linking users to roles, defining which permissions each user inherits from associated roles.

Column	Type
USERNAME	VARCHAR(255)
USER_ROLE_ID	VARCHAR(255)

Keys: - None

Foreign Keys:

- FK_MESSENGER_USER_ROLE_USER → MESSENGER_USER(USERNAME)
- FK_MESSENGER_USER_ROLE_ROLE → USER_ROLE(ID)

22.2.1.4.4. old_password

Keeps track of users' previous passwords for password reuse prevention.

Column	Type
ID	BIGINT
USERNAME	VARCHAR(255)
PASSWORD	VARCHAR(255)

Keys:

- PK_OLD_PASSWORD → (ID, USERNAME)

Foreign Keys:

- FK_OLD_PASSWORD_USERNAME → MESSENGER_USER(USERNAME)

22.2.1.5. Adapters and Integration

Holds information regarding different adapter types which can optionally be used for communication with the backend.

22.2.1.5.1. adapter_info

Describes general adapter settings.

Column	Type
ADAPTER_ID	VARCHAR(50)
MESSENGER_ID	SMALLINT
ADDRESS	VARCHAR(128)
MAXIMUM_THREADS	SMALLINT
PROCESSING_TIMEOUT	INTEGER
FEATURES	VARCHAR(255)

Keys:

- PK_ADAPTER_INFO → (ADAPTER_ID, MESSENGER_ID)

Foreign Keys:

- None directly; referenced by other tables for adapter configuration linkage.

22.2.1.5.2. http_adapter_info

Holds HTTP(S)-specific adapter configuration.

Column	Type
ADAPTER_ID	VARCHAR(50)
PORT	INTEGER
USE_HTTPS	BOOLEAN
PARALLEL_THREADS	INTEGER
PROCESSING_TIMEOUT	INTEGER
ACCEPTED_USER	VARCHAR(30)
RECEIVE_ACK	BOOLEAN
USERNAME	VARCHAR(40)
LAST_CHANGE	TIMESTAMP WITH TIME ZONE

Keys:

- PK_HTTP_ADAPTER → (ADAPTER_ID)

Foreign Keys: - None

22.2.1.5.3. plugable_adapter_config

Stores plugin-based adapter configuration files.

Column	Type
FILENAME	VARCHAR(255)
TIMESTAMP	TIMESTAMP WITH TIME ZONE
DATA	BLOB

Keys:

- PK_PLUGABLE_ADAPTER_CONFIG → (FILENAME)

Foreign Keys: - None

22.2.1.5.4. messenger_add_on_adapter

Stores binaries (jar) and metadata of additional adapters.

Column	Type
FILENAME	VARCHAR(255)
TIMESTAMP	TIMESTAMP WITH TIME ZONE
DATA	BLOB

Keys:

- PK_MESSENGER_MESSENGER_ADD_ONS_ADAPTER → (FILENAME)

Foreign Keys: - None

22.2.1.5.5. messenger_add_on_config

Holds configuration data for additional adapters.

Column	Type
FILENAME	VARCHAR(255)
TIMESTAMP	TIMESTAMP WITH TIME ZONE
DATA	BLOB

Keys:

- PK_MESSENGER_MESSENGER_ADD_ONS_CONFIG → (FILENAME)

Foreign Keys: - None

22.2.1.6. Messenger and System Configuration

Defines overall system configuration, runtime activation, and licensing.

22.2.1.6.1. messenger_activation

Tracks system instances and activation data.

Column	Type
INSTANCE_ALIAS	VARCHAR(255)
INSTANCE_ID	VARCHAR(255)
TIMESTAMP	TIMESTAMP WITH TIME ZONE
USERNAME	VARCHAR(40)
ACTIVATION	BLOB
PRODUCT_KEY	BLOB
PRODUCT_CERT	BLOB
LAST_STARTUP	TIMESTAMP WITH TIME ZONE
IP_ADDRESS	VARCHAR(30)
LAST_HEART_BEAT	TIMESTAMP WITH TIME ZONE
MESSENGER_ID	SMALLINT

Keys:

- PK_MESSENGER_ACTIVATION → (INSTANCE_ALIAS)
- UQ_MESSENGER_ID → (MESSENGER_ID)

Foreign Keys: - None

22.2.1.6.2. messenger_config

Stores general configuration data for messenger components.

Column	Type
TYPE	VARCHAR(30)
TIMESTAMP	TIMESTAMP WITH TIME ZONE
USERNAME	VARCHAR(40)
DATA	BLOB

Keys:

- PK_MESSENGER_CONFIG → (TYPE)

Foreign Keys: - None

22.2.1.6.3. log_message

Stores general events that can occur during messenger process'.

Column	Type
ID	SMALLINT
TYPE	TINYINT
BEGIN_COMPONENT	TINYINT
END_COMPONENT	TINYINT
TEXT	VARCHAR(255)

Keys:

- PK_LOG_MESSAGE → (ID)

Foreign Keys: - None

22.2.1.6.4. global_task

Tracks scheduled or distributed system-level operations. This is a scheduled background functionality of the messenger.

Columns	Type
ID	INTEGER
EXECUTING_MESSENGER_ID	DECIMAL(3)

Keys:

- PK_GLOBAL_TASK → (ID)

Foreign Keys: - None

22.2.1.6.5. messenger_license

Holds software licensing data.

Column	Type
ID	INTEGER
TIMESTAMP	TIMESTAMP WITH TIME ZONE
USERNAME	VARCHAR(40)
LICENSE	BLOB
SERIAL_NUMBER	VARCHAR(50)
CLUSTER_ID	VARCHAR(36)
PRODUCT_KEY	BLOB

PRODUCT_CERT	BLOB

Keys:

- PK_MESSENGER_LICENSE → (ID)

Foreign Keys: - None

22.2.1.7. Supporting Infrastructure

Used by the messenger to track schema migrations and prevent concurrent updates.

22.2.1.7.1. databasechangelog

Databasechangelog holds records of every database change (changeset) executed while migrating the messenger database.

Column	Type
ID	VARCHAR(255)
AUTHOR	VARCHAR(255)
FILENAME	VARCHAR(255)
DATEEXECUTED	TIMESTAMP
ORDEREXECUTED	INTEGER
EXECTYPE	VARCHAR(10)
MD5SUM	VARCHAR(35)
DESCRIPTION	VARCHAR(255)
COMMENTS	VARCHAR(255)
TAG	VARCHAR(255)
LIQUIBASE	VARCHAR(20)
CONTEXTS	VARCHAR(255)
LABELS	VARCHAR(255)
DEPLOYMENT_ID	VARCHAR(10)

Keys: - None

Foreign Keys: - None

22.2.1.7.2. databasechangeloglock

Databasechangeloglock helps to avoid concurrent migration operations in the database.

Columns	Type
ID	INTEGER

LOCKED	BOOLEAN
LOCKGRANTED	TIMESTAMP
LOCKEDBY	VARCHAR(255)

Keys: - PK_DATABASECHANGELOGLOCK → (ID)

Foreign Keys: - None

22.3. Troubleshooting

22.3.1. Unicode-Support

Since version 5.0 the Messenger checks unicode configuration of database on each startup.

The concrete checks depend on current database. [Info Icon] In case the expected match is not found in the configured database the messenger and JDBC logs show warnings /errors related to dbCheck. Please execute the following checks manually in your database and apply the **recommended changes**.

22.3.1.1. MSSQL

```
-- Database uses unicode collation (must contain '_CI_AS' or '_SC')
SELECT collation_name
FROM sys.databases
WHERE name = DB_NAME() AND (collation_name LIKE '%_CI_AS%' OR collation_name LIKE
'%_SC%');
```

22.3.1.2. Oracle

```
-- NLS-Charset should be AL32UTF8
SELECT value FROM nls_database_parameters WHERE parameter = 'NLS_CHARACTERSET';
```

22.3.1.3. PostgreSQL

```
-- Sever-Encoding should be UTF8
SHOW server_encoding;
-- Client-Encoding should be UTF8
SHOW client_encoding;
```

22.3.1.4. MySQL

```
-- Database schema is utf8mb4
SELECT DEFAULT_CHARACTER_SET_NAME FROM INFORMATION_SCHEMA.SCHEMATA WHERE SCHEMA_NAME =
DATABASE();
-- Expected is 1
SELECT COUNT(*) FROM INFORMATION_SCHEMA.SCHEMATA WHERE SCHEMA_NAME = DATABASE() AND
DEFAULT_COLLATION_NAME LIKE 'utf8%';
-- Expected is 0
SELECT COUNT(*) FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = DATABASE() AND
TABLE_COLLATION NOT LIKE 'utf8%';
-- Expected is 0
SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA = DATABASE() AND
CHARACTER_SET_NAME IS NOT null AND CHARACTER_SET_NAME NOT LIKE 'utf8%';
-- Connection character set is 'utf8mb4'
```

```
SELECT @@character_set_connection;
-- Client character set is 'utf8mb4'
SELECT @@character_set_client;
-- Result character set is 'utf8mb4'
SELECT CASE WHEN @@character_set_results IS NULL THEN 'utf8mb4' ELSE
@@character_set_results END
-- Connection collation is 'utf8mb4_unicode_ci'
SELECT CASE WHEN @@collation_connection LIKE 'utf8mb4%' THEN 'utf8mb4' ELSE
@@collation_connection END
```

22.3.2. Partner and Agreement Cache Size

It is possible to adjust the maximum cache size for the partners and agreements in the wrapper.conf if the memory settings or performance requirements for your messenger require you to do so.

```
# Limit for in-memory cache of agreements. Default value is 1000.
set.AGREEMENT_CACHE_LIMIT=1000
# Limit for in-memory cache of profiles. Default value is 1000.
set.PROFILE_CACHE_LIMIT=1000
# Please adjust the id of the following additional properties so that they are unique
in your wrapper.conf
wrapper.java.additional.13=-Dmessenger.cache.agreement.size=%AGREEMENT_CACHE_LIMIT%
wrapper.java.additional.14=-Dmessenger.cache.profile.size=%PROFILE_CACHE_LIMIT%
```

22.3.3. Outbound queue fills up

Messages are stored in the outbound queue and removed when they are successfully delivered or if all transmission attempts have failed.

In normal operation this queue should not fill up, assuming that all destination servers are reachable and not overloaded.

if the queue fills up, this has several implications:

1. the needed memory increases with each queued message
2. the Messenger creates a folder in the filesystem for each message that is about to be transmitted. There might be file system limits on the number of folder that can be created within the work/outbound/ folder
3. startup time of the Messenger will increase with the queue size
4. delivery of messages to same unreachable destination will increase the time until a final result is available for the queued messages.
5. delivery of messages to other destinations are not delayed, but if the overall queue gets too large it will prevent any message processing.

fix **before** Outbound Queue is full:

- prevent new messages to be queued by enabling maintenance mode (reject outbound messages)
- increase max memory in wrapper.conf to allow more messages to be queued
- change filesystem if there is a subdirectory limit (for ex. EXT4 has a limit of 64000 subfolders)
- if one destination is unavailable: in GUI select all outbound messages that are in status "IN TRANSIT" and have an unavailable destination. Then click "delete from queue". This will move all messages to failed archive and set the status to failed.

fix when Outbound Queue is full:

- increase max memory in wrapper.conf to allow Messenger startup to be successful
- DELETE FROM OUTBOUND_QUEUE directly in the DB
  - start Messenger
  - in GUI select all outbound messages that are in status "IN TRANSIT" and click "delete from queue". This will move all messages to failed archive and set the status to failed.
  - resend the failed messages in chunks

22.3.4. Inbound queue fills up

Messages from communication partners are stored in the inbound queue and removed when they are successfully delivered to the configured adapter.
In normal operation this queue should not fill up, assuming that all adapters are running and connected backends accept messages.

if the queue fills up, this has several implications:

1. the needed memory increases with each queued message
2. the Messenger creates a folder in the filesystem for each message that is about to be transmitted. There might be file system limits on the number of folder that can be created within the work/inbound/ folder
3. startup time of the Messenger will increase with the queue size
4. there is no timeout for delivery to adapters, therefore it is important that adapters (and connected backends) are always available

fix **before** the Inbound Queue is full:

- prevent new messages to be queued by enabling maintenance mode (reject inbound messages). However this will cause errors at the senders.
- increase max memory in wrapper.conf to allow more messages to be queued
- change filesystem if there is a subdirectory limit (for ex. EXT4 has a limit of 64000 subfolders)
- if an adapter (or it connected backend) is unavailable, messages should be "deleted from the inbound queue" using the GUI

fix when Inbound Queue is full:

- increase max memory in wrapper.conf to allow Messenger startup to be successful

- DELETE FROM INBOUND_QUEUE directly in the DB
  - start Messenger
  - in GUI select all inbound messages that are in status "IN TRANSIT" and click "delete from queue". This will move all messages to failed archive and set the status to failed.
  - resend the failed messages in chunks after the adapter (and connected backend) are working

22.3.5. Required database rights

Dedicated rights are needed for each database system dedicated to operational and update mode. Replace placeholders [database_name], [schema_name] and [app_user] in the scripts below with the relevant values for database, schema and database user.

22.3.5.1. MS-SQL

22.3.5.1.1. Update-Mode

```
GRANT ALTER ON DATABASE::[database_name] TO [app_user];
GRANT CONTROL ON DATABASE::[database_name] TO [app_user];
GRANT SELECT, INSERT, UPDATE, DELETE TO [app_user];
```

22.3.5.1.2. Operational-Mode

```
REVOKE CONTROL ON DATABASE::[database_name] FROM [app_user];
REVOKE ALTER ON DATABASE::[database_name] FROM [app_user];
-- Only reduced DML rights
GRANT SELECT, INSERT, UPDATE, DELETE TO [app_user];
```

22.3.5.2. Oracle

22.3.5.2.1. Update-Mode

```
GRANT CREATE TABLE TO [app_user];
GRANT ALTER ANY TABLE TO [app_user];
GRANT DROP ANY TABLE TO [app_user];
GRANT CREATE SEQUENCE TO [app_user];
GRANT DROP ANY SEQUENCE TO [app_user];
GRANT CREATE SESSION TO [app_user];
ALTER USER [app_user] quota unlimited on USERS;
```

22.3.5.2.2. Operational-Mode

```
REVOKE CREATE TABLE FROM [app_user];
REVOKE ALTER ANY TABLE FROM [app_user];
REVOKE DROP ANY TABLE FROM [app_user];
```

```
REVOKE CREATE SEQUENCE FROM [app_user];
REVOKE DROP ANY SEQUENCE FROM [app_user];
GRANT CREATE SESSION TO [app_user];
ALTER USER [app_user] quota unlimited on USERS;
```

22.3.5.3. MySQL

22.3.5.3.1. Update-Mode

```
GRANT REFERENCES, ALTER, CREATE, DROP, INDEX, INSERT, UPDATE, DELETE, SELECT ON
[database_name].* TO '[app_user]'@'%';
```

22.3.5.3.2. Operational-Mode

```
REVOKE REFERENCES, ALTER, CREATE, DROP, INDEX ON [database_name].* FROM '[app_user]'@
'%';
-- Only reduced DML rights
GRANT SELECT, INSERT, UPDATE, DELETE ON [database_name].* TO '[app_user]'@'%';
```

22.3.5.4. PostgreSQL

22.3.5.4.1. Update-Mode

User must be owner of table to alter it

```
GRANT CREATE, USAGE ON SCHEMA [schema_name] TO [app_user];
GRANT ALL ON ALL TABLES IN SCHEMA [schema_name] TO [app_user];
GRANT ALL ON ALL SEQUENCES IN SCHEMA [schema_name] TO [app_user];
GRANT ALL ON ALL FUNCTIONS IN SCHEMA [schema_name] TO [app_user];
```

22.3.5.4.2. Operational-Mode

```
GRANT CONNECT ON DATABASE [database_name] TO [app_user];
GRANT USAGE ON SCHEMA [schema_name] TO [app_user];
GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA [schema_name] TO
[app_user];
GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA [schema_name] TO [app_user];
```

22.3.6. Manual database setup/update

During setup of PONTON X/P Messenger a shell-script is installed (**sql/dbupdateTool.bat** (Windows-Batch) or **sql/dbupdateTool** (Linux Bash-Script)). This script can be used to get current structural status of database and run the update manually. This script supports the following command parameters:

parameter	description
status	Prints a list of undeployed changesets, which will be deployed during update process.
update	Runs the structural update of database, manually.
updateScript	Generates a native SQL Script, containing all required structural updates for current Messenger DB. This can be executed manually by database admin f.e. This is the recommended way to update the database, if the database user Messenger uses, doesn't have admin rights on database.
snapshot	Dumps a snapshot of current database structure. This contains a description of all database objects, but no content.
listLocks	List currently locked database objects. This may happen, if a update process fails.
releaseLocks	Releases all locked database objects, to rerun update process after failure. This command should NOT be used thoughtless. If structural update of database fails, the case and the current state of database must be analyzed properly to return to a consistent database again.
listActivations	(since 5.0.0) Lists all activation records from messenger database.
deleteActivation *#instanceAlias#*	(since 5.0.0) Deletes the activation record, defined by given instanceId, to allow startup of messenger with a license without enabled ClusterMode.
resetAdminAccount	(since 5.0.0) Resets the 'xpadmin' account to factory settings. If user does not exist, it will be created.

22.3.6.1. Example: dbupdateTool update

```
cd ./sql
./dbupdateTool update
```

```
Start update of DB structure on
jdbc:hsqldb:file://git/messenger/xpmessenger/target/dist/data/database/xpmsglog
Juli 26, 2024 10:07:43 AM liquibase.database INFORMATION: Set default schema name to
PUBLIC
Juli 26, 2024 10:07:43 AM liquibase.changelog INFORMATION: Reading from
PUBLIC.DATABASECHANGELOG Database is up to date, no changesets to execute
Juli 26, 2024 10:07:43 AM liquibase.changelog INFORMATION: Reading from
PUBLIC.DATABASECHANGELOG UPDATE SUMMARY Run: 0 Previously run: 30 Filtered out: 0
------------------------------- Total change sets: 30
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: UPDATE SUMMARY
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: Run: 0
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: Previously run: 30
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: Filtered out: 0
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: -------------------------------
```

```
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: Total change sets: 30
Juli 26, 2024 10:07:43 AM liquibase.util INFORMATION: Update summary generated
Juli 26, 2024 10:07:44 AM liquibase.lockservice INFORMATION: Successfully released
change log lock
Juli 26, 2024 10:07:44 AM liquibase.command INFORMATION: Command execution complete
```

PONTON GmbH

Dorotheenstraße 64

22301 Hamburg

Germany

Web: http://www.ponton.de

LinkedIn https://www.linkedin.com/company/ponton-consulting/