



PONTON
WE ARE THE 2 IN B2B

X/P Messenger 3.11.0

Version: 41

Date: 23-Mar-2021

Copyright Notice



This document is the confidential and proprietary information of PONTON GmbH ("Confidential Information"). You shall not disclose such Confidential Information and shall use it only in accordance with the terms of the license agreement you entered into with PONTON GmbH.

Table of Contents

1.	Further Information and Support.....	6
1.1.	Technical Support/Helpdesk.....	6
1.2.	PONTON GmbH.....	6
1.3.	General Information	6
2.	Introduction to PONTON X/P	7
2.1.	Introduction	7
2.1.1.	About PONTON X/P	7
2.2.	Architectural Overview	7
2.3.	Supported Features	8
2.3.1.	Basic Features	8
2.3.2.	Security Features	8
3.	Downloading the Software	10
3.1.	Components.....	10
4.	Installing PONTON X/P	11
4.1.	Installation procedure.....	11
4.1.1.	Windows	11
4.1.2.	Linux/UNIX.....	12
4.2.	Importing the X/P configuration from a previous version	14
4.2.1.	Messenger Version < 3.1	14
4.2.2.	Messenger Version 3.1 - 3.6	14
4.2.3.	Messenger Version 3.7 and up.....	15
5.	Quick-Starting the Software	16
5.1.	Logging in	16
5.1.1.	Using the Menu/Navigation Panel.....	17
5.1.2.	Activate the software (trial version)	17
5.2.	Basic configuration	19
5.2.1.	Define a local partner.....	19
5.2.2.	Define remote partners	22
5.2.3.	Set up a partner agreement	23
5.3.	Start communication	24
5.3.1.	Check your proxy settings	24

5.3.2.	Send a Ping message.....	24
5.3.3.	Overview in message monitor	26
6.	Configuration Options	28
6.1.	Messenger Configuration	28
6.1.1.	Messenger Database.....	28
6.1.2.	Logging Level.....	30
6.1.3.	Message Queue Settings.....	30
6.1.4.	Partner Registry Configuration	31
6.1.5.	E-mail Configuration	33
6.1.6.	E-mail Notification.....	35
6.1.7.	Communication Settings	37
6.1.8.	Time Server Configuration	41
6.1.9.	Server configuration.....	42
6.1.10.	Archive Settings	45
6.1.11.	Activation / License Configuration.....	47
6.1.12.	Maintenance.....	50
6.2.	Listener Settings.....	51
6.3.	CA Certificates	51
6.4.	Hot Folder Adapter (HFA)	52
6.4.1.	General Configuration.....	52
6.4.2.	Create / Delete Hot Folder	52
6.4.3.	Configuring an Hot Folder Adapter	53
6.5.	Global Schema Configuration.....	59
6.5.1.	Adding a new SchemaSet.....	60
6.6.	User Administration	61
6.6.1.	Password Policy	62
6.6.2.	Password expiry	63
6.6.3.	Account locking	63
6.7.	Import Configuration	63
6.8.	Partner Configuration.....	64
6.8.1.	Create a Partner Entry	64
6.8.2.	Delete a Partner Entry	75
6.8.3.	Using the Partner Registry	75
6.9.	Partner Agreements.....	76
6.9.1.	Creating a Partner Agreement.....	77

6.9.2.	Editing a Partner Agreement	78
7.	Advanced Configuration.....	87
7.1.	Listener Configuration.....	87
7.1.1.	Listener Installation.....	87
7.1.2.	Listener Settings in the Messenger Admin Tool.....	87
7.1.3.	FTP Settings	90
7.1.4.	Server Certificate.....	92
7.1.5.	Client Certificate	93
7.1.6.	Installing partner certificate on the Listener	93
7.2.	Set Messenger instance name	94
7.3.	Messenger Cluster mode	94
7.4.	Application Monitoring (JMX).....	94
7.4.1.	Monitoring Partner Connection	95
7.5.	Advanced Database Configuration	95
7.5.1.	Installing other Databases.....	96
7.6.	XML Schema Configuration.....	96
7.6.1.	Defining a new Schema Set	96
7.6.2.	Extending an existing Schema Set	97
7.7.	Uploading a new Schemaset.....	98
7.8.	Advanced Message Monitor Configuration	99
7.9.	Agreement Configuration for Plain Packager.....	100
7.9.1.	Outbound Configuration	100
7.9.2.	Inbound Configuration.....	101
7.10.	Content Rules	102
7.11.	Partner Certificates.....	104
7.11.1.	LDAP Certificate Import	104
7.12.	Data Extraction from XML documents	104
7.12.1.	XPATH Types	105
7.12.2.	Envelope Mapping.....	106
7.12.3.	Payload Mapping.....	106
8.	Troubleshooting	108
8.1.	Locating Inconsistencies in a Partner Agreement	108
8.2.	Port Configuration.....	109
8.2.1.	HTTP Settings.....	109

- 8.3. Identification of Message-Type..... 110
- 9. Supported Crypto Algorithms 111**
 - 9.1. EbXML20 Packager..... 111
 - 9.2. AS1/AS2/AS3 Packager..... 111
 - 9.3. AS4 Packager 112
 - 9.4. Messenger 2.1 Payload Processor 113
 - 9.5. SSL/TLS..... 113

1. Further Information and Support

1.1. Technical Support/Helpdesk

<https://support.ponton.de>

Phone:

+49 40 866275 344

1.2. PONTON GmbH

Homepage:

<https://www.ponton.de/>

Postal Address:

Dorotheenstrasse 64
22301 Hamburg
Germany

1.3. General Information

For in-depth Information regarding the widely used communication standards and protocols please refer to the following documentation:

Link	Description
http://www.w3.org/	World Wide Web Consortium
https://www.oasis-open.org/standards	OASIS standards organization
http://www.ebxml.org	Regarding ebXML
http://www.ietf.org	Regarding AS1 , AS2 und AS3
http://www.xml.org	XML industry portal
www.ntp.org	NTP (Network Time Protocol)

2. Introduction to PONTON X/P

2.1. Introduction

2.1.1. About PONTON X/P

PONTON X/P is the **ebXML, AS1, AS2, AS3 and AS4 compliant Message Service** developed by PONTON GmbH. It ensures encrypted, signed, compressed, validated, archived, and guaranteed transfer of messages between business partners. PONTON X/P supports HTTP, HTTPS, SMTP, SMIME, FTP and FTPS protocols.

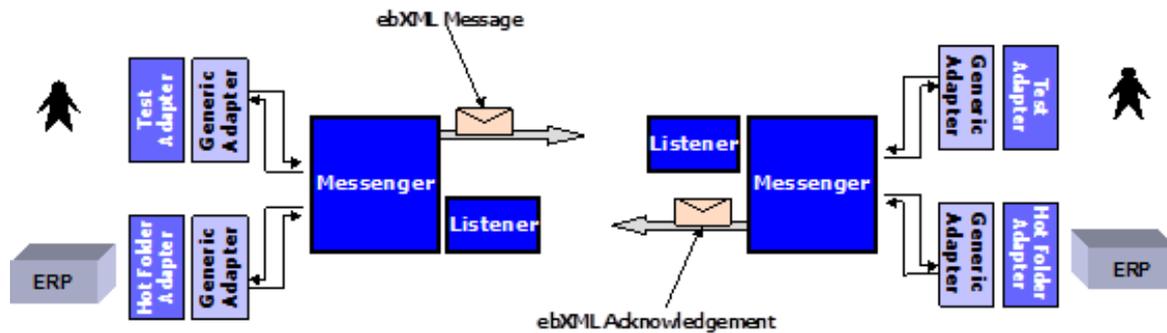
PONTON X/P can also be installed as a service within your internal Network within minutes. PONTON X/P is packaged with an **embedded HSQL database** and web server, so that the installation & test process only requires very few configuration steps. The Message Service also includes use of the **PONTON Certificate Authority**, which is integrated into the Messenger and supported by PONTON GmbH. If users of PONTON X/P prefer migration to **third-party certificate authorities** such as VeriSign®, Thawte®, or GlobalSign® this can easily be done just by requesting and installing the corresponding certificate.

Integrating the PONTON X/P in a variety of **backend applications** is made effectively possible and flexible based on a large range of adapters from PONTON or third parties.

2.2. Architectural Overview

PONTON X/P consists of the following main modules:

1. **Messenger** – This is the core of PONTON X/P. It transforms messages received from the back-end (for example an ERP system) into a standard-compliant ebXML messages. Several processing steps are performed within the messenger before the ebXML message is sent to the receiver.
2. **Listener** – This (optional) module is usually located in the DMZ to receive message from remote systems and forward them to the Messenger within the secure zone of an organization. No further processing is carried out by the Listener. A distributed installation, with the Listener installed separately from the Messenger, is not necessary if the Messenger is in the DMZ or if it is used for internal integration.
3. **Adapter** – There are many ways to integrate the Messenger with the application software in the back-end. An adapter helps bridge this gap. There are different adapters available for use with PONTON X/P: PONTON X/D is a Database Adapter that maps XML payload content directly to and from a database. The Hot Folder Adapter scans outbox folders and transfers documents to the Messenger. Vice-versa, messages received from a business partner are dropped into an inbox folder.



2.3. Supported Features

2.3.1. Basic Features

Feature	
EbXML 2.0	✓
AS1, AS2, AS3, AS4	✓
reliable message delivery	✓
XML message validation	✓
EDIFACT, X12 messages	✓
content extraction from messages	✓
database and file log	✓
audit trail	✓
max. payload document size	1GB
>92% document compression	✓
archiving of documents and signatures	✓
notification by emails	✓
web based configuration and monitoring	✓
programming interface for software integration	✓
online registry for partner profile exchange	✓

2.3.2. Security Features

Feature	
---------	--

Feature	
end-to-end encryption	
end-to-end persistent signatures	
channel encryption	
channel authentication	
SMIME support	
X509 certificate management	
1-click signature verification	

3. Downloading the Software

The software can be downloaded from the PONTON homepage.

For the required link, please contact the helpdesk at <https://support.ponton.de>

3.1. Components

You will find the following components in the installation package:

- **PONTON X/P Messenger** – the core component for guaranteed, secure delivery of messages
- **PONTON X/P Hot Folder Adapter** – allows easy connection of the Messenger to your application software
- **HTTP Adapter** – allows HTTP-based back-end integration with your backend system(s).
- **Test Adapter** – allows direkt upload of Files from your Filesystem into the Messenger
- **PONTON X/P Listener** – a lightweight process to receive documents via HTTP or FTP and forward them to your Messenger over the firewall.
- **E-mail Listener** – another lightweight process that polls your mail server for new messages.

4. Installing PONTON X/P

4.1. Installation procedure

4.1.1. Windows

The PONTON X/P messenger is installed on a **Windows** operating system using a self-extracting executable, which guides the user through the installation process. If only standard options are chosen, the installation process takes approximately 10 minutes.

To Install the PONTON X/P Messenger take the following steps:

Step 1: Start the installation by double-clicking the PONTON X/P setup file. A Setup Guide will show on your screen and help you navigate through the installation.

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:

Code Block 1 Service installer configuration in launcher\confwrapper.conf

```
set.MESSENGER_NAME="set value in wrapper.conf"  
# this value will be displayed in the web GUI to identify the Messenger instance  
set.NTSERVICE_NAME=pontonexpmessenger  
# 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.
```

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

It is highly recommended to make the following preparations in the the database before running the service:

1) The required database tables have been defined in the database schema. Suitable SQL scripts are provided in the folder 'sql' within the messenger installation.

2) 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

4.1.2. Linux/UNIX

The 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/UNIX machine with the user intended to run the messenger. Ensure that this user has the right to read, write and 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 3.x/pontonxp** as well as the **PONTON XP 3.x/launcher/linux-.../wrapper** files are executable.

Step 3 : Configure the necessary parameters in pontonxp :

Code Block 2 Installation configuration in pontonxp

```
...
APP_HOME="." # Ensure that this location refers to your PONTON
XP 3.x messenger installation.
...
```

Defining a suitable name for your messenger:

Code Block 3 Defining the messenger name in launcher/conf/wrapper.conf

```
set.MESSENGER_NAME="set value in wrapper.conf"
```

Step 4 : Before starting the PONTON X/P Messenger please set up your database

Messenger database preparations

It is highly recommended to make the following preparations in the the database before running the service:

- 1) The required database tables have to defined in the database schema. Suitable SQL scripts have been provided in the folder 'sql' within the messenger installation.
- 2) 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 5 : Start the messenger service

- Manual start

```
./pontonxp start
```

Alternatively:

- Control start/stop using systemd

Many current Linux distributions come with systemd replacing the old SysVinit script based service launcher.

This textfile in the right place plus the command `# systemd daemon-reload` registers the PONTON X/P Messenger as a systemd service :

Code Block 4 /etc/systemd/system/pontonxp.service

```
[Unit]
Description=PONTON XP
After=network-online.target

[Service]
Type=forking
# Put user with write permissions below
User=username
# Put absolute path to pontonxp base-directory in all of the following
PIDfile=[path_to_pontonxpdir]/launcher/conf
ExecStart=[path_to_pontonxpdir]/pontonxp start
ExecStop=[path_to_pontonxpdir]/pontonxp stop

[Install]
WantedBy=multi-user.target
```

- 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

```
# systemctl enable pontonxp
```

The command above enables the pontonxp service over reboots.

Use `systemctl status pontonxp` to obtain runtime informations and log. `systemctl stop pontonxp` shuts down the messenger.

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

4.2. Importing the X/P configuration from a previous version

4.2.1. Messenger Version < 3.1

Configurations from Messenger Versions older than 3.1 are not compatible with the current version. Please contact our helpdesk to discuss your upgrade path.

4.2.2. Messenger Version 3.1 - 3.6

The configuration files and database content are compatible with the current Messenger version. However there was a change in the directory structure, therefore it is required to copy the old files to the correct folder as listed below:

- Copy and replace the following folders or files from the Installation Path of the old messenger (XP_OLD) into the Installation folder of new Messenger (XP_NEW)
- **Copy the Database Driver** file from the Installation path `<XP_OLD>\xmlpipe\lib_ext` into Installation path `<XP_NEW>\lib_ext`
- **Rename** the existing Config folder under Installation path `<XP_NEW>\config` into **config_NotInUse**
- **Copy the Config folder** from the `<Installation path <XP_OLD>\xmlpipe\config` into Installation path `<XP_NEW>\config`

- **Copy the Archive folder** from the <Installation path <XP_OLD>\xmlpipe\archive into Installation path <XP_NEW>\data\archive
- **Copy the Archive_failed** folder from the <Installation path <XP_OLD>\xmlpipe\archive_failed into Installation path <XP_NEW>\data\archive_failed
- **Copy the Hotfolder** folder from the <Installation path <XP_OLD>\xmlpipe\<hotfolder name> into Installation path <XP_NEW>\data\<hotfolder name>
- Stop the old Messenger (XP_OLD)
- Start the new Messenger (XP_NEW)

4.2.3. Messenger Version 3.7 and up

The configuration files and database content are compatible with the current Messenger version. The following folders can be copied as needed :

- Copy and replace the following folders or files from the Installation Path of the old messenger (XP_OLD) into the Installation folder of new Messenger (XP_NEW)
- **Copy the Database Driver** file from the Installation path <XP_OLD>\lib_ext into Installation path <XP_NEW>\lib_ext
- **Rename** the existing Config folder under Installation path <XP_NEW>\config into **config_NotInUse**
- **Copy the Config folder** from the <Installation path <XP_OLD>\config into Installation path <XP_NEW>\config
- **Copy the Archive folder** from the <Installation path <XP_OLD>\data\archive into Installation path <XP_NEW>\data\archive
- **Copy the Archive_failed** folder from the <Installation path <XP_OLD>\data\archive_failed into Installation path <XP_NEW>\data\archive_failed
- **Copy the Hotfolder** folder from the <Installation path <XP_OLD>\data\<hotfolder name> into Installation path <XP_NEW>\data\<hotfolder name>
- Stop the old Messenger (XP_OLD)
- Start the new Messenger (XP_NEW)

5. Quick-Starting the Software

After following the 'Installation procedure' as described in the previous Section your messenger should now be successfully started and ready for further configuration.

5.1. Logging in

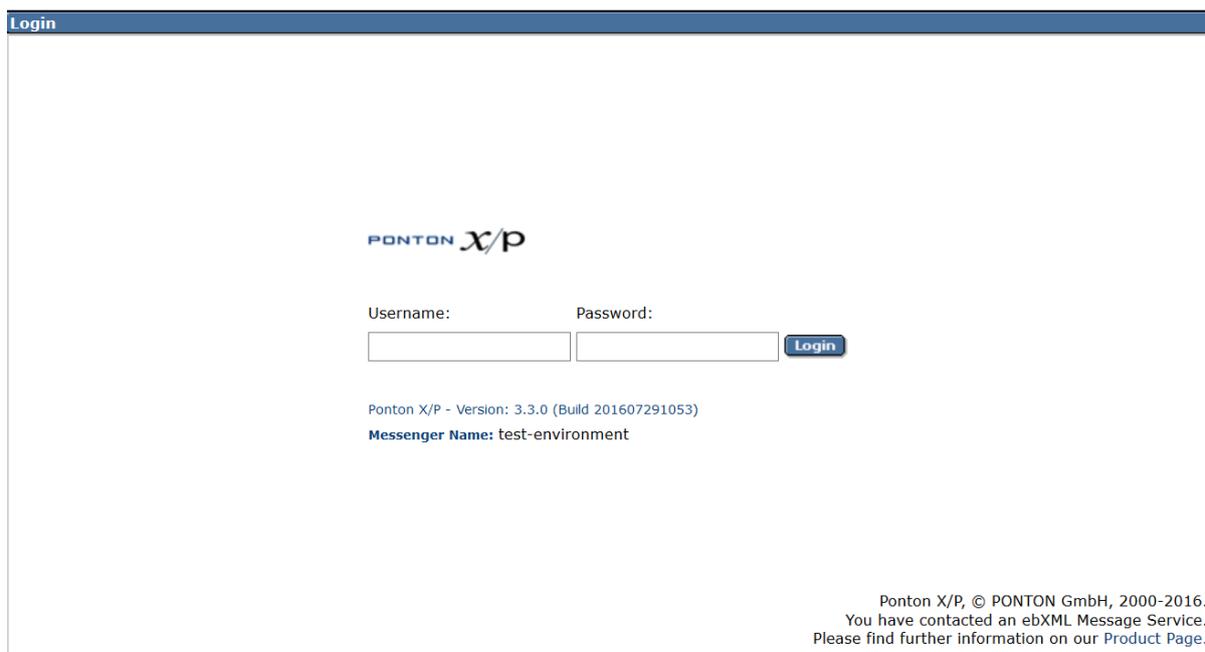
Open your web browser and enter the URL :

`https://<hostname>:8443/pontonxp`

or

`https://localhost:8443/pontonxp` 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 screenshot shows a web browser window titled "Login". The main content area features the "PONTON x/p" logo at the top center. Below the logo, there are two input fields: "Username:" and "Password:". To the right of the "Password:" field is a blue "Login" button. Below the input fields, the text "Ponton X/P - Version: 3.3.0 (Build 201607291053)" and "Messenger Name: test-environment" is displayed. In the bottom right corner, there is a small copyright notice: "Ponton X/P, © PONTON GmbH, 2000-2016. You have contacted an ebXML Message Service. Please find further information on our Product Page."

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

for an on premise installation these are the default values:

User: xadmin

Password: xppass

for an AWS installation these are the default values:

User: xadmin

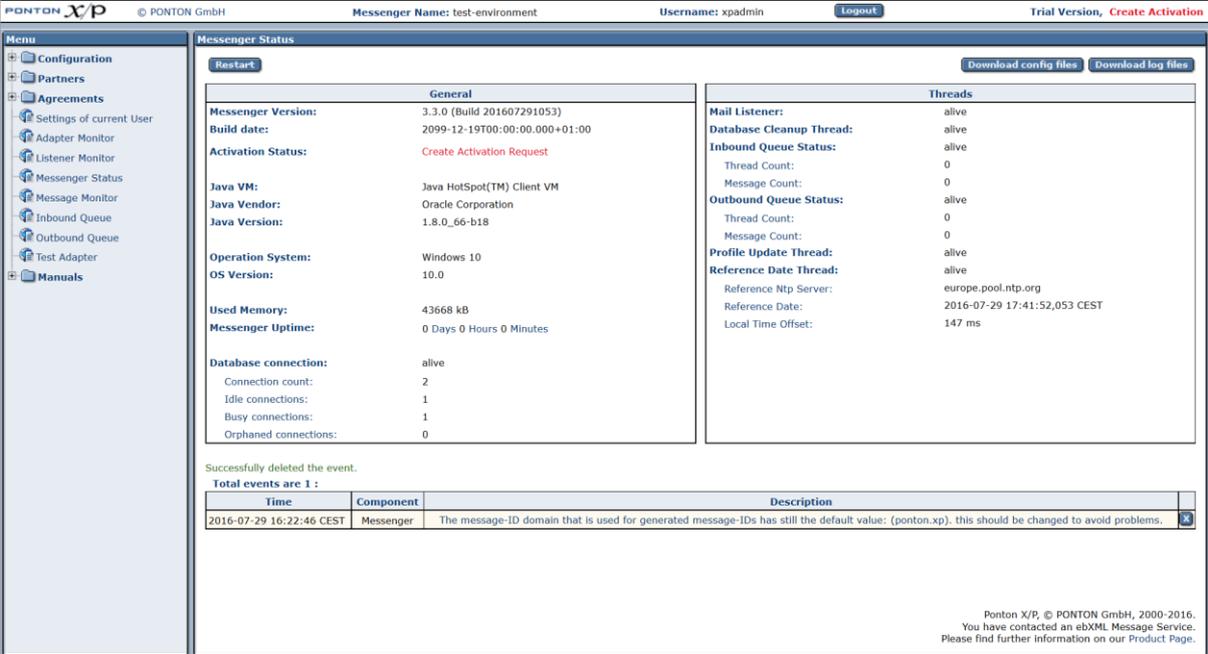
Password: (EC2 instance_id)

Important

Since these initial user login values have to be changed on first login to prevent unauthorized access to the Administration Tool.

By default web browsers are allowed to store the username and password values, please have a look at chapter 7.5 if you want to prevent this

On startup, the Messenger status screen is displayed, showing information on the current server configuration and the status of different Messenger processes (Threads). You can switch to this screen at any time by choosing Messenger Status from the menu.



PONTON X/P © PONTON GmbH Messenger Name: test-environment Username: xpadmin Logout Trial Version, Create Activation

Menu: Configuration, Partners, Agreements, Settings of current User, Adapter Monitor, Listener Monitor, Messenger Status, Message Monitor, Inbound Queue, Outbound Queue, Test Adapter, Manuals

Messenger Status

Restart Download config files Download log files

General		Threads	
Messenger Version:	3.3.0 (Build 201607291053)	Mail Listener:	alive
Build date:	2099-12-19T00:00:00.000+01:00	Database Cleanup Thread:	alive
Activation Status:	Create Activation Request	Inbound Queue Status:	alive
Java VM:	Java HotSpot(TM) Client VM	Thread Count:	0
Java Vendor:	Oracle Corporation	Message Count:	0
Java Version:	1.8.0_66-b18	Outbound Queue Status:	alive
OS Version:	Windows 10	Thread Count:	0
Used Memory:	43668 kB	Message Count:	0
Messenger Uptime:	0 Days 0 Hours 0 Minutes	Profile Update Thread:	alive
Database connection:	alive	Reference Date Thread:	alive
Connection count:	2	Reference Ntp Server:	europe.pool.ntp.org
Idle connections:	1	Reference Date:	2016-07-29 17:41:52,053 CEST
Busy connections:	1	Local Time Offset:	147 ms
Orphaned connections:	0		

Successfully deleted the event.

Total events are 1:

Time	Component	Description
2016-07-29 16:22:46 CEST	Messenger	The message-ID domain that is used for generated message-IDs has still the default value: (ponton.xp), this should be changed to avoid problems.

Pontoon X/P, © PONTON GmbH, 2000-2016. You have contacted an eXML Message Service. Please find further information on our Product Page.

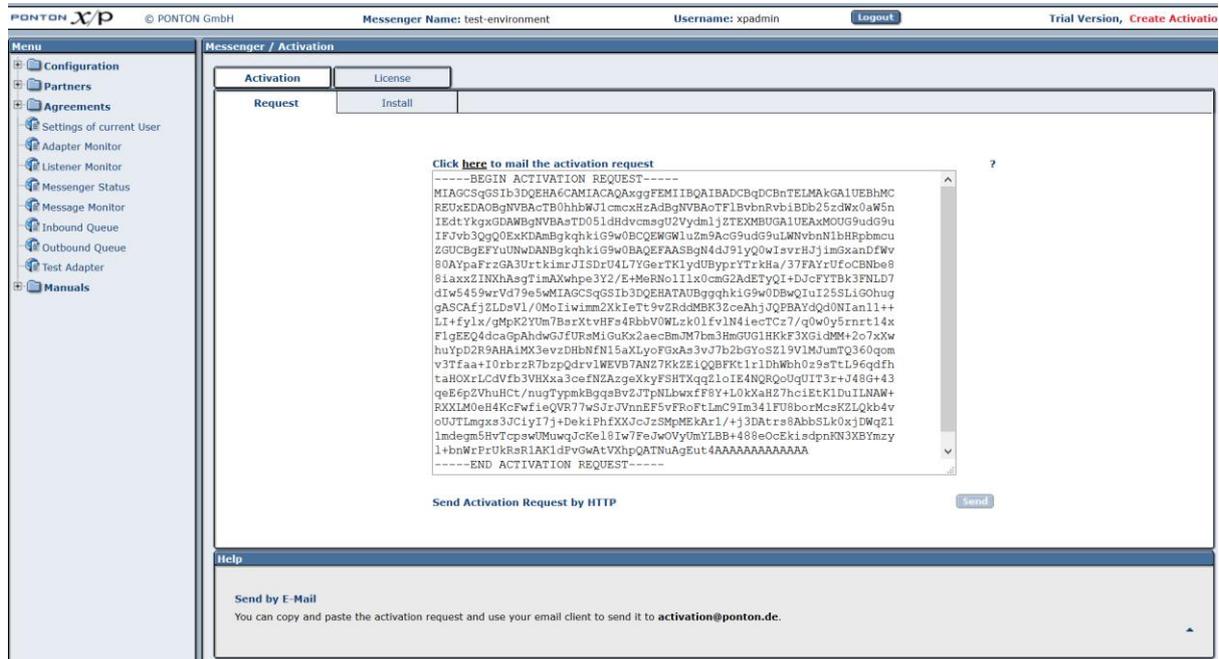
5.1.1. Using the Menu/Navigation Panel

Click on the icons  in the menu panel to navigate to the specific folders. Click on the page labels to display the corresponding screens.

5.1.2. Activate the software (trial version)

Before proceeding to the communication tests it is important to activate your messenger. You can run PONTON X/P Messenger as a trial version for upto 60 days. To activate the trial version go to **Configuration > Messenger > Activation/License** and click on the Activation Request tab or simply click the Create Activation Request link shown on the

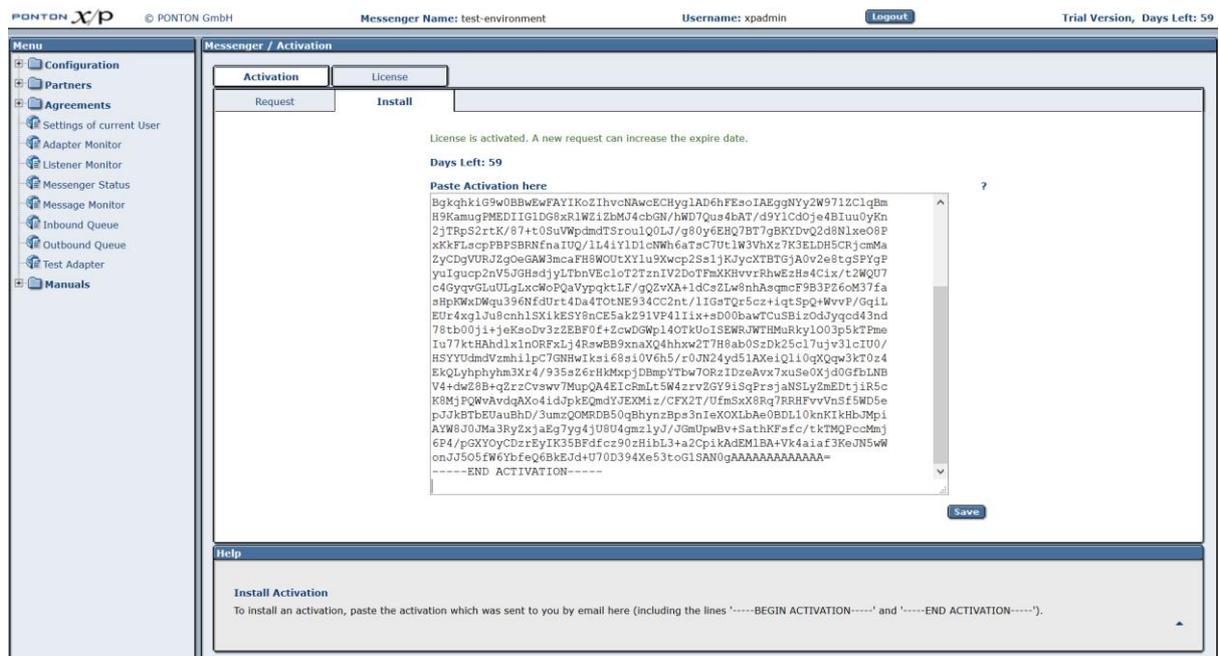
startup screen (Messenger Status). This will call up the Activation Request tab with a box containing your activation request.



For the trial version, please click on the e-mail link at the top of the page. This will copy the activation request to your e-mail client. Using your e-mail client, please send the activation request to activation@ponton.de.

Note: The Send Activation Request by HTTP option is only available when activating a license and is therefore disabled in the trial version.

You will receive a reply e-mail containing the activation code for your system. Please copy the *complete activation code* and paste it into the text box on the Install tab:



Note

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 -----". This is also the case when copying the activation code from the reply e-mail into the Install tab. Again, please be sure to include the "Begin" and "End" lines.

5.2. Basic configuration

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

- a *local partner* (representing your own organization)
- a *remote partner* (representing your business partner's organization)

Of course, for your actual daily business you will generally exchange messages with a number of different business partners, so you might need to define different remote partner configurations.

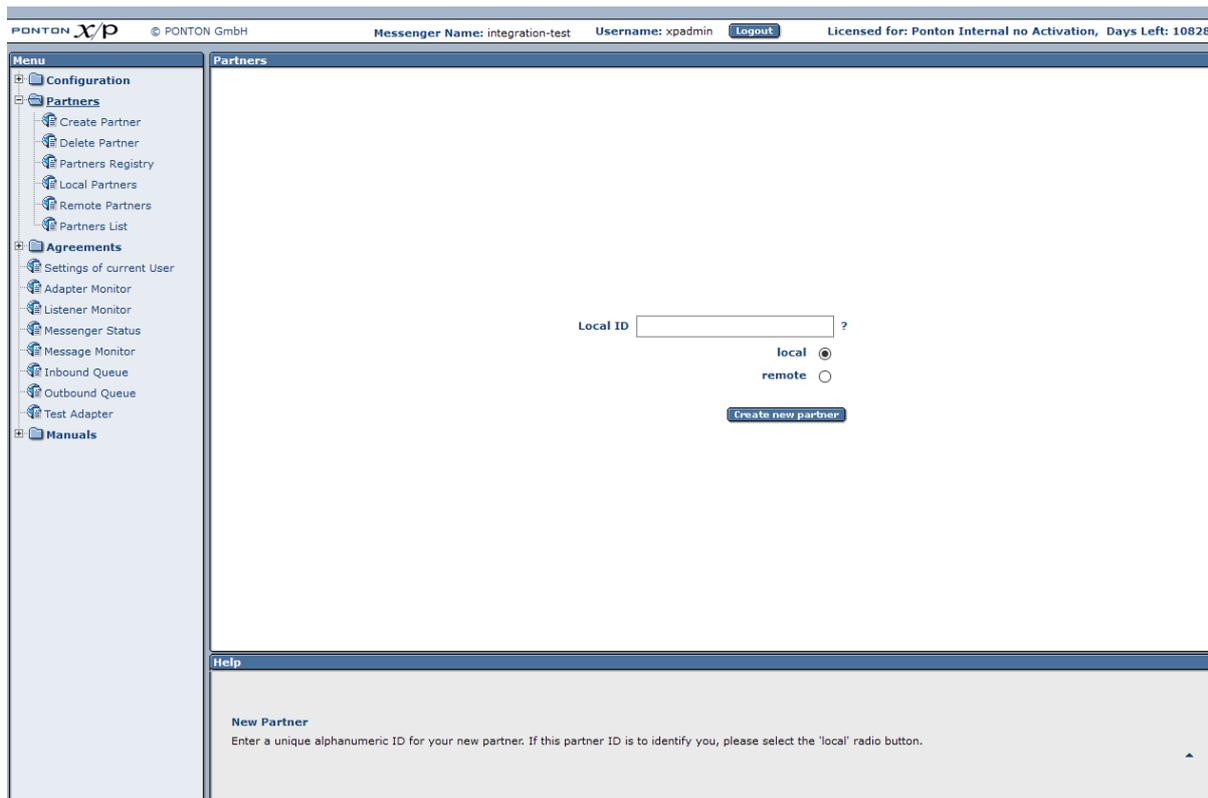
Recommendation to set up a test installation first

It is useful to set up an initial test installation preferably in a test environment. It is often easier to install two Messengers on separate PCs within your local environment to avoid firewall restrictions. On the other hand, 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.

5.2.1. Define a local partner

Step 1: Create a local partner

Open the Configuration menu and navigate to **Partners > Create Partners**. On the Create Partners screen, enter a **Local ID** for yourself, and activate the **local** radio button in order to create a local partner. Then click **Create New Partner**.



The next step is to specify the configuration details for this new partner. You can edit an existing partner configuration afterwards by navigating to **Configuration > Partners > Local Partners** and selecting your partner name from the drop down menu at the top of the page. When you create a new partner, the Local Partner Configuration screen is displayed with the new partner name selected automatically. There are different tabs for the various configuration settings: Identification, Communication, Schema Sets, etc.

Step 2: Identification settings

On the **Identification** tab, 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 Internal Partner ID and the PartyIDs are all set to the same value as the Local ID used when a new partner is created. In the Identification tab you can modify these settings as required.

- **Partner Display Name** – the Display Name is used within PONTON X/P in menus, selection lists, etc.
- **Internal Partner ID** – the Internal Partner ID is used for communication with the backend (ERP) system.

- **PartyID** – the PartyID is used for the identification of business partners in the messaging process. Please note that the PartyIDs at the senders end must match the PartyIDs at the receivers end.

Click **Save** to confirm your settings.

Step 3: Communication settings

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`

Step 4: Message content settings

In the **Schema Sets** tab, indicate which schema sets you wish to support. This will indicate which message types are supported by your partner.

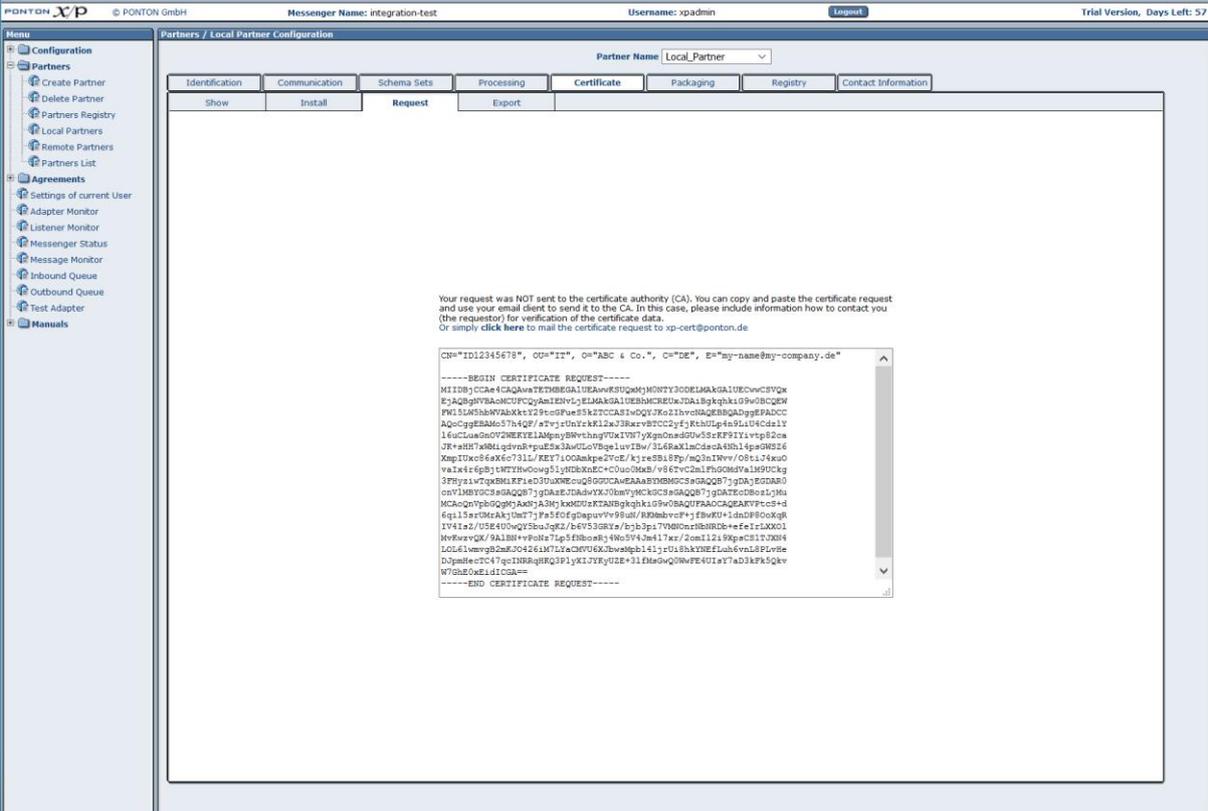
Step 5: Certificates

PONTON X/P enables you to send signed and/or encrypted messages based on the use of certificates.

The successful use of certificates is only possible if the sender as well as the receiver have installed the respective partner certificates in their respective messaging software. You may choose to **skip** this step for your initial tests. In that case, please note that the following settings have to be modified to compensate for the absence of certificates:

- In the Tab Processing **deactivate** the **Signing** and **Encryption** options
- In the Tab Packaging **deactivate** the **Use XML Signature** option for **EbXml**

Configuration for actual business purposes should include certificates for your local and remote partners. PONTON offers a lightweight certificate authority (CA) that allows you to easily request and install certificates for the Messenger. The **Certificate** tab has further tabs for requesting, installing and subsequently exporting a certificate (for a local partner). To request a certificate from the PONTON CA, click on the **Request** tab and fill in the certificate request form.



Partners / Local Partner Configuration

Partner Name: Local Partner

Identification Communication Schema Sets Processing **Certificate** Packaging Registry Contact Information

Show Install **Request** Export

Your request was NOT sent to the certificate authority (CA). You can copy and paste the certificate request and use your email client to send it to the CA. In this case, please include information how to contact you (the requestor) for verification of the certificate data.
Or simply [click here](#) to mail the certificate request to xp-cert@ponton.de

```

-----BEGIN CERTIFICATE REQUEST-----
MIIDBjCCAc4CAQAwTEYwBGlUEAAwR3UQkYMONTY3ODEMAGALUECvuwCSVQx
EjAqBgNVBAMwCUPQc2AiZmVjLjE1MAKGA1UEBmMCRDkzDk1Bkgkqki9w0BCQEM
FVU1MABhMVAkXzI3P00P0eS3LZFCAL1eQVJRo2Il1w0tqgBq2dngpEADCC
AQoCqgEBAmeS7kqW4eTvjU5VzK1L2w3Rae+8TCC2fjKtMjU46P1U4CdaIY
16uCLoa0sOV2WEKVELAMpY8NvtngVUX1VN7YXgnOnad0Uv5SEKFFIY1vtP82oa
JR+eHTa9M1g0vsh+puE5a3wUoVbqeluvlBw/3L69axJmCdaCA4Nb14psGMS16
Wap1W0568X673LlFEY1000akpe2Y0Z/kjreS18Pp/q2a1NwV/0S119xw0
V4I4r6Bj1WZYfu00v951yNDbKkEC+0u0Nxb/+987vC2m1F8S0M9V41M90CKg
3F8y1v7qgBMLKFAed3UdX0N6+uqS97UCwEAA8PDM8MCSsGAQQB7jgDAjEGDAR0
cnV1MhUChsR0Q087jgDAEJ3k4dYK1U8vF9K3C380AQ087jgDAEcc08e1j9Ma
WCaQp0q0q9+8a0J3NtKdM0uKZAN8qkbt1G9v8AUF0A0C28AP7eFcd+
6q15s10MzAkjUm77jPa5f0fgDapuvV98uM/R8Mbvof+jEbwKU+1dnP80oKqR
1V41a2/U5E410wQV38u3qZ/b6V53GR1z/bj03p17W80nrMBNRD6+eFe1rX001
Wf8vrgW/SAL8H+P0k71q580Bm08j4W0V4Um11az/Com112189pe0117084
LOLE1vmpg2m2J04E6M7LxCM7U6JbwaMpb141jU18kYNEFL6h6vL8PLv8e
Dj38e0c7C47q0INB8gRQ3P1yK1J78YUZE+31E8a9wQ0WFE4U1e7ad3kFK5kv
W78E0e01d10d8=
-----END CERTIFICATE REQUEST-----
  
```

 For further details on working with certificates see the *Partner Certificates* section.

5.2.2. Define remote partners

To test your Messenger configuration, a remote partner will be required.

Step 1: Create a remote partner

Open the Configuration menu and navigate to **Partners > Create Partners**. On the Create Partners screen, enter Local ID = **PontonXPTestServer** and activate the **remote** radio button in order to create a remote partner. Then click **Create New Partner**.

Step 2: Communication settings

Click the tab Communication and enter the URL for the test server hosted by PONTON and **Save** the changes.

<https://xptest.ponton-consulting.de/pontonxp/SoapListener>

Step 3: Message content settings

In the **Schema Sets** tab, choose the schema sets your partner is ready to accept.

Step 4: Certificates

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.

- In the Tab Processing deactivate the **Signing** and **Encryption** options
 - **Save** the changes
- In the Tab Packaging deactivate the **Use XML Signature** option for **EbXml**

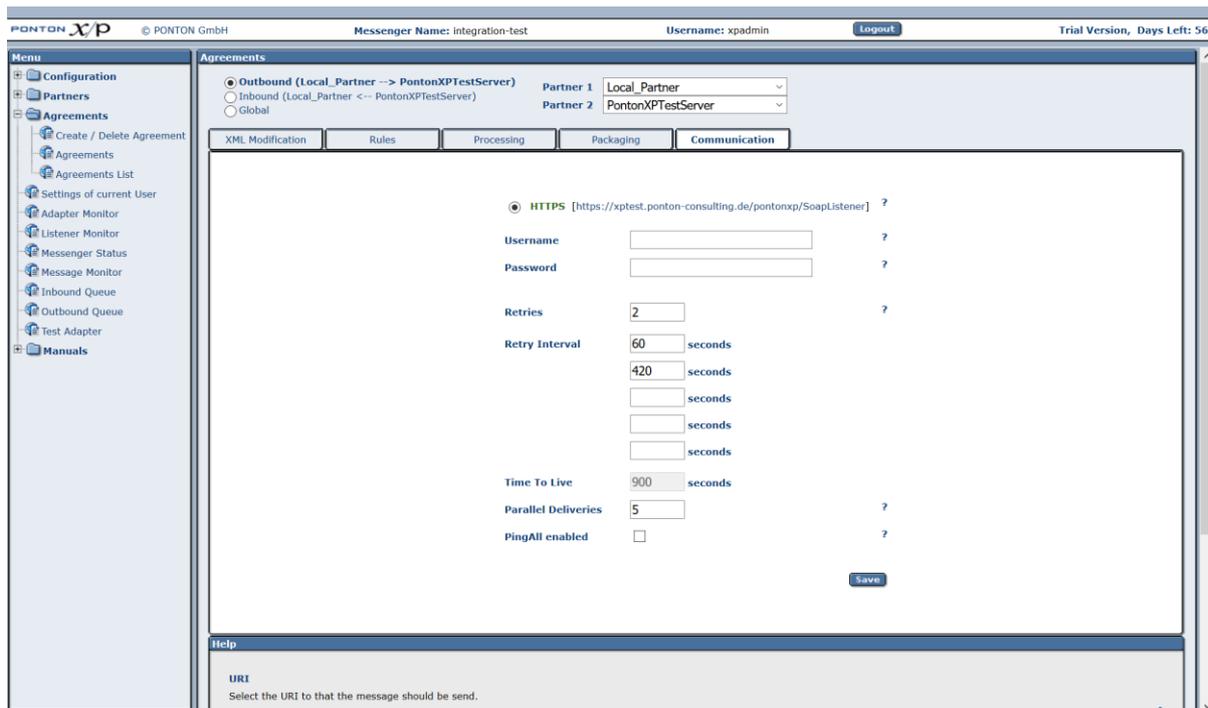
Note: When exchanging partner configurations with your business partners please keep in mind that *identical party IDs have to be used in the local and remote configurations*. The partner display names and internal IDs, on the other hand, may be different.

	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

5.2.3. Set up a partner agreement

Now that both local as well as remote partner set up is ready the next step is to define an agreement between these two partners. Thus allowing them to successfully communicate with each other.

Open the Configuration menu and navigate to **Agreements > Create/Delete Agreement**. On the Create/Delete Agreement screen, choose **create**. Then choose **your local Partner ID** as Partner 1 and **PontonXPTestServer** as Partner 2 from the list of available partners. Click **Create New Agreement**.



The screenshot shows the PONTON X/P Messenger configuration interface. The top bar displays 'PONTON X/P', '© PONTON GmbH', 'Messenger Name: integration-test', 'Username: xpadmin', and 'Logout'. The main area is titled 'Agreements' and shows an 'Outbound (Local_Partner --> PontonXPTestServer)' agreement. The 'Partner 1' is 'Local_Partner' and 'Partner 2' is 'PontonXPTestServer'. The 'Communication' tab is selected, showing the following configuration:

- HTTPS [https://xptest.ponton-consulting.de/pontonxp/SoapListener] ?
- Username: ?
- Password: ?
- Retries: ?
- Retry Interval: seconds
- seconds
- seconds
- seconds
- Time To Live: seconds
- Parallel Deliveries: ?
- PingAll enabled: ?

A 'Save' button is located at the bottom right of the configuration area. A 'Help' section at the bottom left contains the text: 'URI Select the URI to that the message should be send.'

 For further details on partner agreements see the *Partner Agreements* section.

5.3. Start communication

5.3.1. 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 the section - *Listener Configuration*.

5.3.2. 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. The Test Adapter can be started by simply choosing the **Test Adapter** from the navigation bar. This will lead you to a new tab in your browser:

PONTON XP © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Trial Version, Days Left: 56

Search:

Sender: Local_Partner

Receiver: PontonXPTestServer

Test Message

Ping Ping All Status

File on Server

Send message

Local file

Durchsuchen... Keine Datei ausgewählt.

Send message

Incoming / Outgoing Messages

Time	Message ID	Sender	Receiver	Direction	Message Type	Test	Status	Conversation ID
2016-08-02 13:19:31 CEST	MID-1470136642608@ponton.xp	Local_Partner	PontonXPTestServer	OUT	PING		Message successfully sent.	MID-1470136642608@ponton.xp

Message:::

Step 1: Choose the sender and receiver

Step 2: Click Ping

This will send an EbXml Ping message to the chosen receiver. If your Ping message could reach the receiver and he recognizes your partner the response should be a **Pong message**. A Pong message does not ensure that your firewall allows incoming messages from your business partner. To verify that please see step 3.

Step 3: Send your partner a test message

To send a test message or file to your partner using the test adapter:

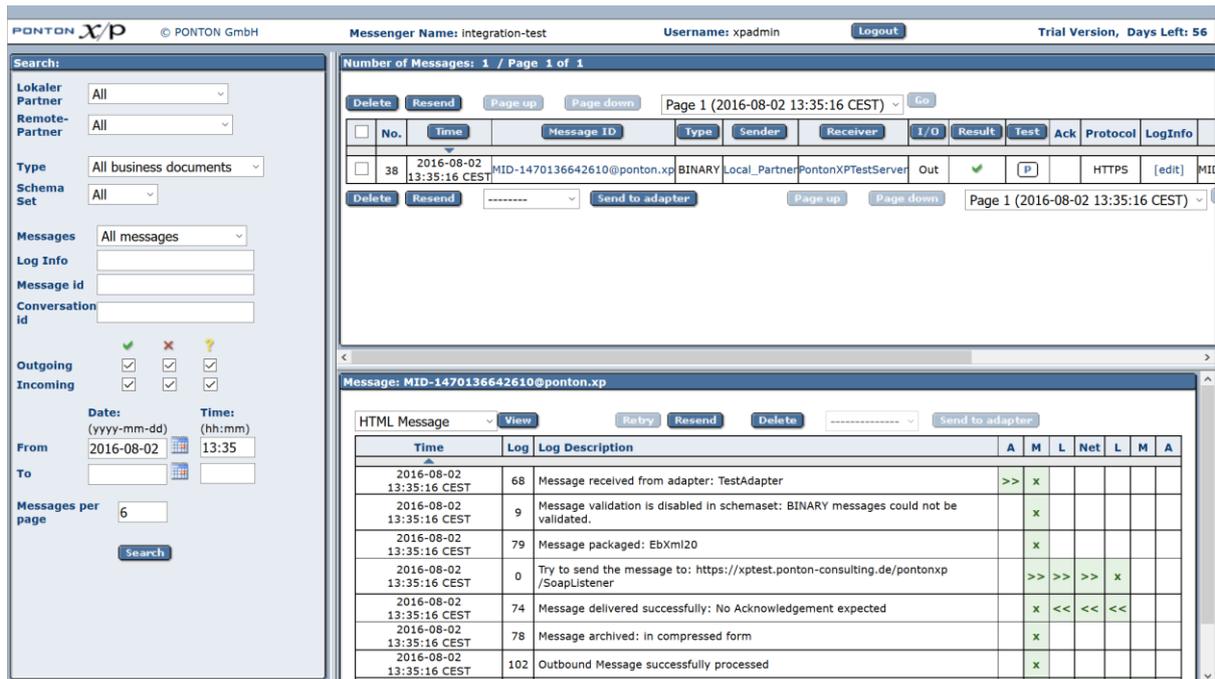
- Select a document (from the **File on server** list or by choosing a **Local file**)
- It is optional to activate the **Test Message** checkbox
- Send the document by clicking **Send Message**

The document is then processed by your messenger and sent 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 your partner to deliver the messages to your messenger successfully then the message delivery should be shown as successful.

5.3.3. Overview in message monitor

Messages sent and/or received by your messenger can be shown in the message monitor. Click the **Message monitor** on the navigation bar and this shall lead you to a new Tab in your browser. You could choose to search for specific messages on the basis of their IDs, transmission dates or status. Click **search** to show you the list of messages that match your criteria.

To see detailed information about these messages click the **message ID** in the overview. A detailed list of events will be shown for the chosen message.



The screenshot shows the PONTON X/P Messenger interface. The top bar includes the logo, version (3.11.0), messenger name (integration-test), username (xpadmin), and a trial version notice. The left sidebar contains search filters. The main area shows a list of messages, with one selected and its details expanded in a lower panel. The details panel shows a log of events for the selected message, including successful delivery and processing.

The following color codes are used to indicate the transfer/processing status:

- Green checkmark – the transfer was successful.
- Red cross – something went wrong (in this case, the complete entry is highlighted red).
- Question mark – the message is still unconfirmed (in this case, the entry is highlighted yellow).

To check for details, click on the MessageID and look at the log information (in the lower right panel). Each processing step carried out by your Messenger is displayed here. As long as no errors occurred, the log entries are highlighted green.

The left-hand columns in the details block show:

- How the message was transferred from your test adapter to the Messenger
- Which Messenger filters were applied to the message
- How the document was transferred to the receiver

The right-hand columns in the details block indicate the processing sequence:

A	M	L	Net	L	M	A
Sender's Adapter	Sender's Messenger	Sender's Listener	Network/Internet	Receiver's Listener	Receiver's Messenger	Receiver's Adapter

6. Configuration Options

The overall configuration of Ponton X/P breaks down into the following sections:

- [Messenger configuration](#). This section focuses on local setting of your Messenger. This includes database connections, default filter settings, communication protocol selection etc.
- [Partner configuration](#). Per partner, several settings are required: partner identification, filter activation (which overrides the default setting), communication settings, etc.
- [Agreement configuration](#). To communicate, two partners need to agree on a set of settings, they want to use for the interchange.
- [Certificate management](#). For own partners, key pairs may be created and certificates requested. For certificate authorities as well as for each individual partner, certificates can be installed. Certificates may be requested for signing and encryption, for SSL, and for S/MIME.
- [Hot folder configuration](#). The Hot Folder Adapter is tightly integrated with the Messenger and can therefore be configured through the same interface. It supports the definition of multiple hot folders for sending and receiving documents as well as dedicated folders for business partners.

6.1. Messenger Configuration

6.1.1. Messenger Database

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

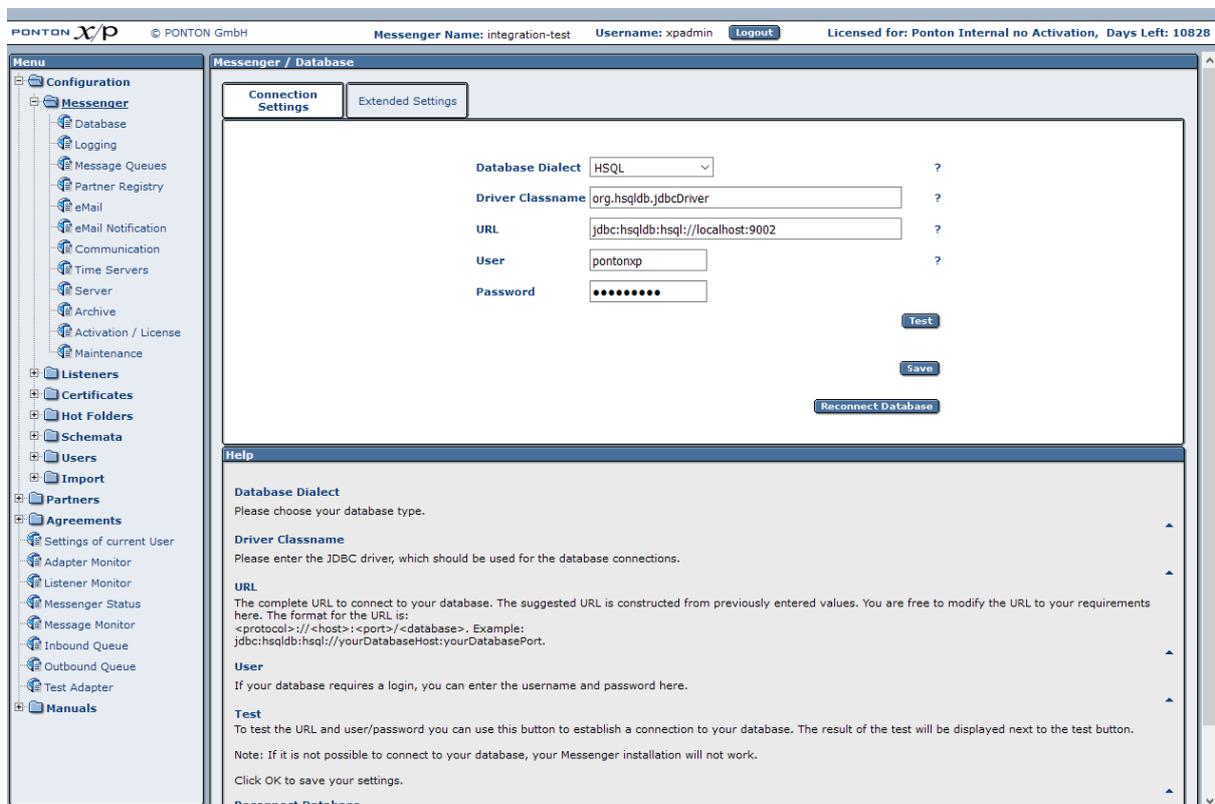
PONTON X/P is installed with a pre-configured HSQL database. **Please note, that the HSQL database is intended only for test purposes.** For productive operations a compatible database system as described under the Section '[Installing other Databases](#)' should be used.

The log database is accessed via JDBC connection. The PONTON X/P distribution includes configuration scripts to set up the tables for the database systems mentioned above. You can refer to these scripts as examples to create scripts for your own database system.

If you do not yet have a database system with JDBC support in use, you can download the setup files for MySQL from <http://dev.mysql.com/downloads>.

To configure the Messenger database please take the following steps:

1. In the Messenger Configuration → Messenger → Database.
2. Choose the required Database dialect from the dropdown list.
3. Enter the driver class name.
4. Enter the URL for the JDBC connection to your database.
5. Enter the user name and password for the connection, if required.
6. Click **Test** to test the connection.
7. Click **Reconnect database** to connect to the new database.



The screenshot shows the 'Messenger / Database' configuration page. The 'Connection Settings' tab is active. The form contains the following fields:

- Database Dialect:** HSQL (dropdown menu)
- Driver Classname:** org.hsqldb.jdbcDriver
- URL:** jdbc:hsqldb:hsq://localhost:9002
- User:** pontonxp
- Password:** [masked with dots]

Buttons for 'Test', 'Save', and 'Reconnect Database' are visible. A 'Help' section at the bottom provides instructions for each field:

- Database Dialect:** Please choose your database type.
- Driver Classname:** Please enter the JDBC driver, which should be used for the database connections.
- URL:** The complete URL to connect to your database. The suggested URL is constructed from previously entered values. You are free to modify the URL to your requirements here. The format for the URL is: <protocol>://<host>:<port>/<database>. Example: jdbc:hsqldb:hsq://yourDatabaseHost:yourDatabasePort.
- User:** If your database requires a login, you can enter the username and password here.
- Test:** To test the URL and user/password you can use this button to establish a connection to your database. The result of the test will be displayed next to the test button. Note: If it is not possible to connect to your database, your Messenger installation will not work. Click OK to save your settings.

Note

The connection to the standard HSQL database supplied with the Messenger requires a "truncated" URL that does not contain the database name (as shown above). When using a different database system, please consult the relevant driver documentation for details on how to specify the database URL.

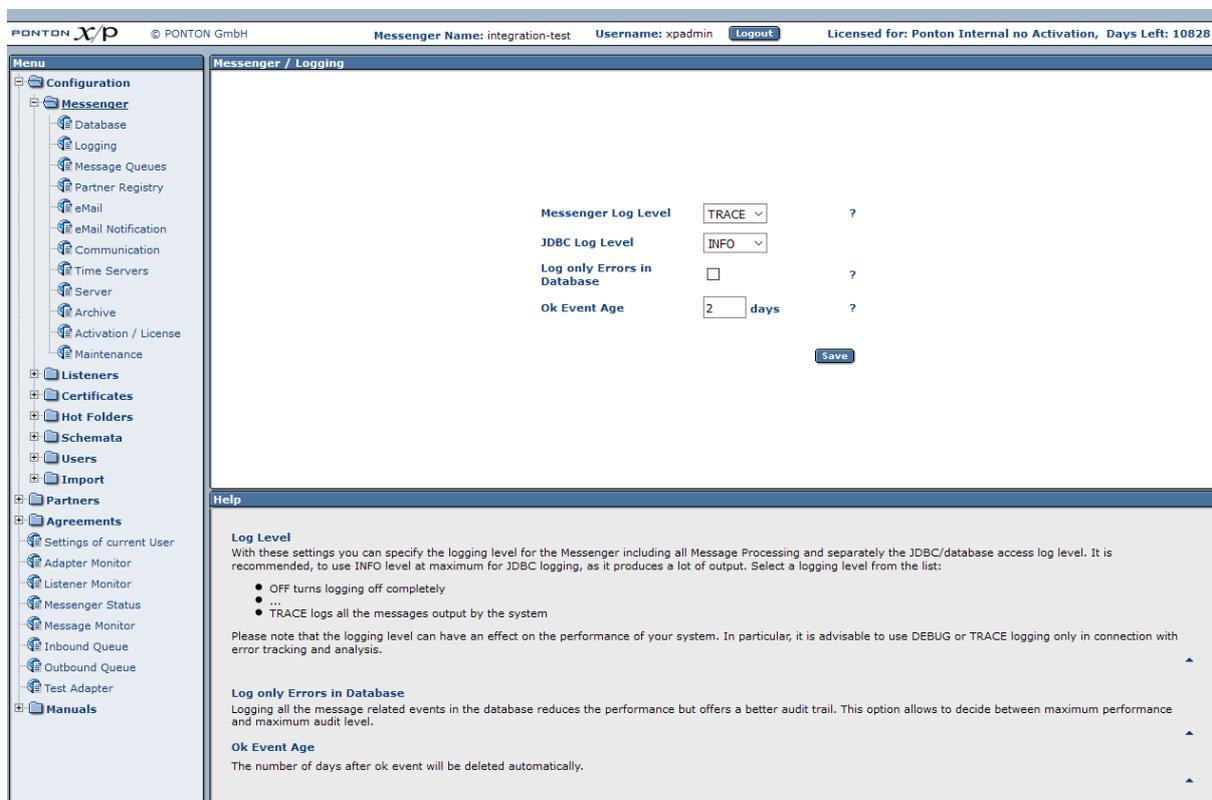
6.1.2. Logging Level

To specify the logging level, go to Configuration → Messenger → Logging and select the desired settings for Messenger and JDBC logging.

There is a range of settings available:

- OFF turns logging off completely.
- ...
- TRACE logs all the messages output by the system.

Note: 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.



The screenshot shows the X/P Messenger configuration interface. The top navigation bar includes the PONTON logo, copyright information (© PONTON GmbH), Messenger Name (integration-test), Username (xpadmin), a Logout button, and license information (Licensed for: Ponton Internal no Activation, Days Left: 10828). The left sidebar contains a menu with categories like Configuration, Listeners, Certificates, Hot Folders, Schemata, Users, Import, Partners, and Agreements. The main content area is titled 'Messenger / Logging' and contains the following settings:

- Messenger Log Level: TRACE (dropdown menu)
- JDBC Log Level: INFO (dropdown menu)
- Log only Errors in Database: (checkbox)
- Ok Event Age: 2 days (input field)

A 'Save' button is located at the bottom right of the settings area. Below the settings is a 'Help' section with the following text:

Log Level
 With these settings you can specify the logging level for the Messenger including all Message Processing and separately the JDBC/database access log level. It is recommended, to use INFO level at maximum for JDBC logging, as it produces a lot of output. Select a logging level from the list:

- OFF turns logging off completely
- ...
- TRACE logs all the messages output by the system

Please note that the logging level can have an effect on the performance of your system. In particular, it is advisable to use DEBUG or TRACE logging only in connection with error tracking and analysis.

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
 The number of days after ok event will be deleted automatically.

6.1.3. Message Queue Settings

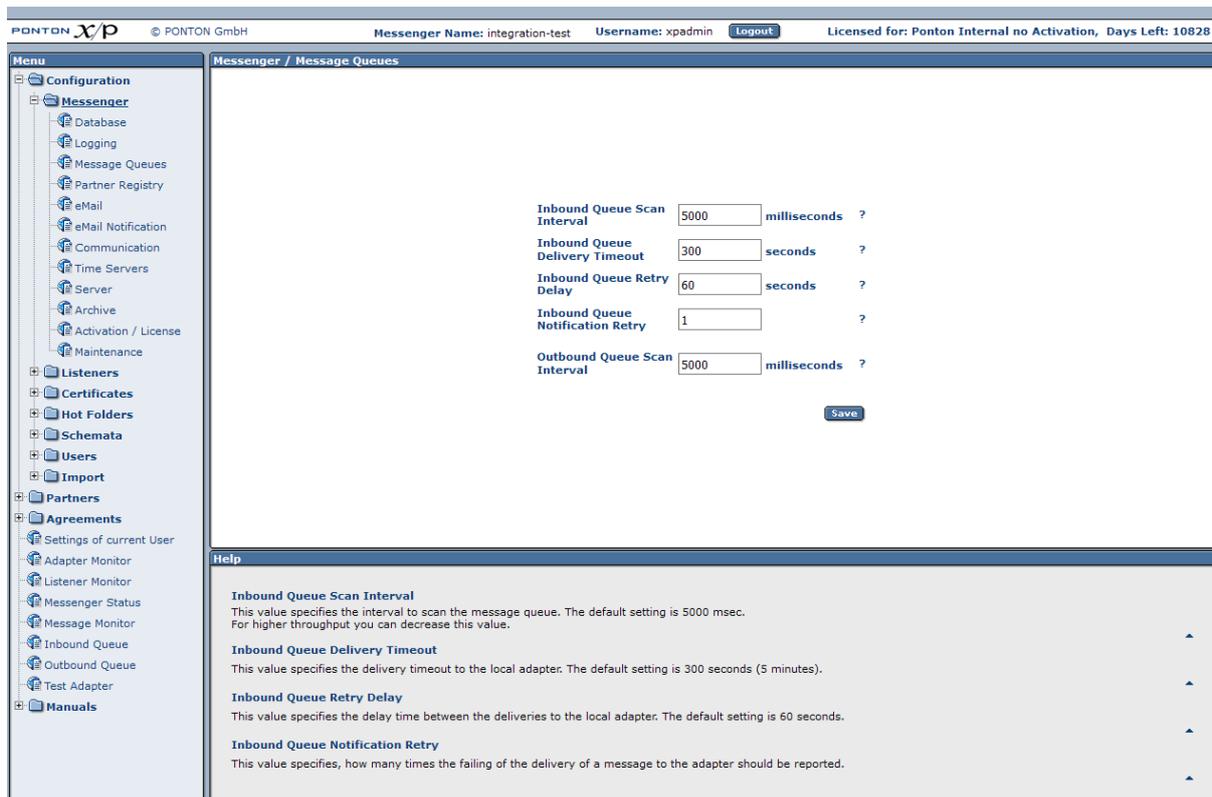
Under Configuration → Messenger → Message Queues you can specify the interval to scan the (inbound and outbound) message queues.

The **Inbound Queue Delivery Timeout** specifies the maximum timeframe allowed for a successful message delivery to an adapter. The timeframe starts when a message is scheduled for delivery and ends when the adapter acknowledges the correct reception. Whenever this allowed timeframe is exceeded a warning message will be logged. In

combination with the email notification this can be used to alert an administrator about the communication issue between Messenger and Adapter.

With the **Inbound Queue Notification Retry** you can configure, how many times the failing of the delivery of a message to the adapter should be reported. So if the delivery timeout is specified as 5 minutes, a warning will be created every 5 minutes.

Inbound Queue Retry Delay specifies the delay after an unsuccessful message delivery attempt. This is used to disburden the receiving adapter in case of load peaks.



The screenshot shows the configuration page for 'Message Queues' in the PONTON X/P Messenger. The interface includes a top navigation bar with the product name, version, and user information. A left-hand menu lists various configuration categories. The main content area contains several settings for message queues, each with a text input field, a unit dropdown, and a help icon. A 'Save' button is located at the bottom right of the settings area. Below the settings is a 'Help' section with detailed descriptions for each parameter.

Setting	Value	Unit
Inbound Queue Scan Interval	5000	milliseconds
Inbound Queue Delivery Timeout	300	seconds
Inbound Queue Retry Delay	60	seconds
Inbound Queue Notification Retry	1	
Outbound Queue Scan Interval	5000	milliseconds

Help

- Inbound Queue Scan Interval**
This value specifies the interval to scan the message queue. The default setting is 5000 msec. For higher throughput you can decrease this value.
- Inbound Queue Delivery Timeout**
This value specifies the delivery timeout to the local adapter. The default setting is 300 seconds (5 minutes).
- Inbound Queue Retry Delay**
This value specifies the delay time between the deliveries to the local adapter. The default setting is 60 seconds.
- Inbound Queue Notification Retry**
This value specifies, how many times the failing of the delivery of a message to the adapter should be reported.

6.1.4. Partner Registry Configuration

The partner registry allows you to exchange profiles with other partners by uploading and downloading partner configurations to/from a central registry. The connection and authentication to access the registry are configured on this page under Configuration → Messenger → Partner Registry.

- **Registry URL** – enter the address where the registry is to be accessed
 - Please note that modifying the registry URL is only possible after activating the checkbox besides it.
- **Username/Password** – enter the user name and password for access to the registry. These will be provided by the 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 registry.
- **Automatic profile updates** – this option allows your messenger to automatically update the already imported profiles at a specified interval. Please note that the download interval is only enabled when automatic updating is active.
- **Automatic partner creation** – this option allows your messenger to automatically create profiles at runtime. The Messenger will try to find a partner profile in the registry based on the internal-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 this 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 partners now** – click on the **Download** button to update your imported profiles immediately.

Note

While updating the partner certificates from the registry the client certificates on the listener are also updated automatically.

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10828

Menu

- Configuration
 - Messenger
 - Database
 - Logging
 - Message Queues
 - Partner Registry
 - eMail
 - eMail Notification
 - Communication
 - Time Servers
 - Server
 - Archive
 - Activation / License
 - Maintenance
 - Listeners
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Messenger / Partner Registry

Registry URL ?

Username ?

Password ?

Automatic agreement updates ?

Automatic profile updates ?

Automatic partner creation ?

Automatic partner cleanup ?

Download interval hours ?

Synchronize partner now ?

Help

Registry URL
The URL to the partner registry.

Username
The username of messenger in the partner registry.

Password
The password of the user.

Automatic agreement updates
If a partner is automatically updated from the registry server and this option is enabled, all agreements with the partner will be updated automatically.

Automatic profile updates
Enable automatic updates of the partners.

Automatic partner creation
If enabled, the messenger creates unknown partners from partner registry to process incoming and outgoing messages.

6.1.5. E-mail Configuration

By setting up inbound and outbound e-mail connections in your Messenger configuration you can enable a number of useful options, in particular:

- [E-mail notification](#) – this requires an outbound e-mail connection.
- [SMTP and SMIME protocols](#) – the use of SMTP and/or SMIME as a transport protocols requires an outbound e-mail connection for sending messages and an inbound e-mail connection for receiving messages.

Note

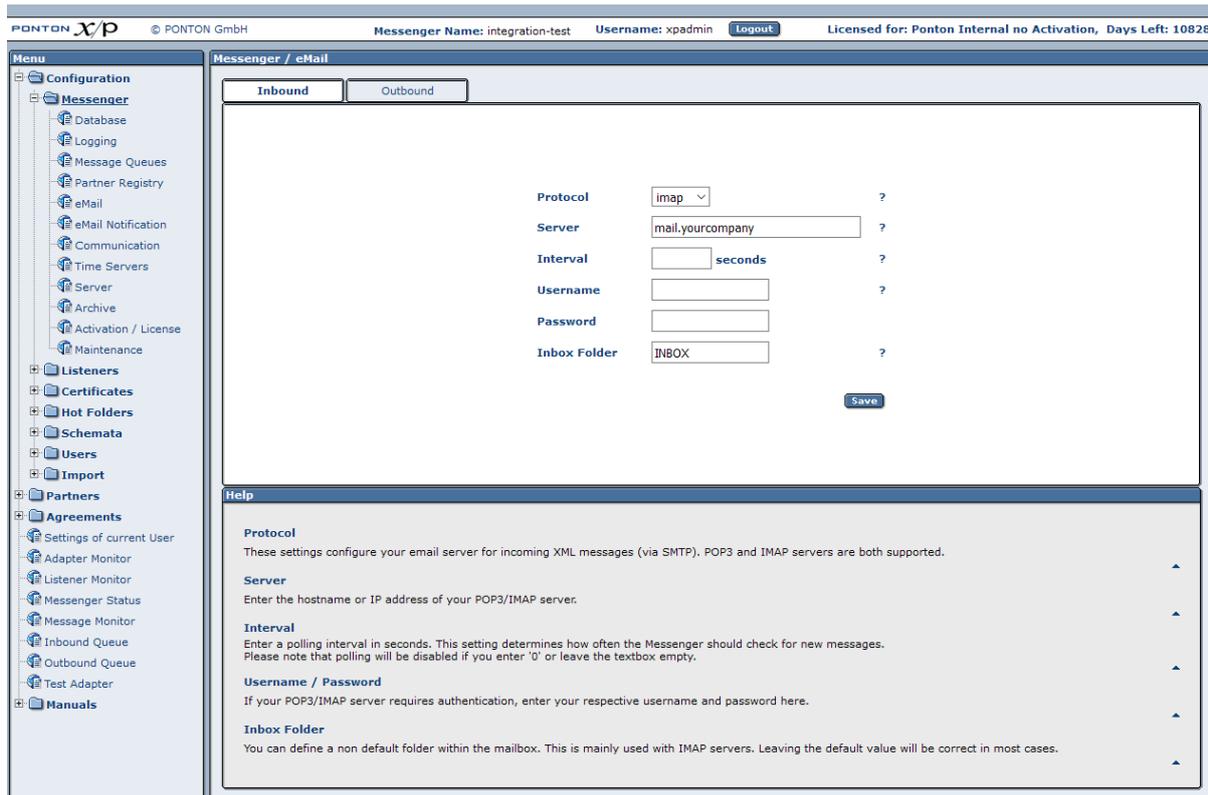
Email Configuration is a must before being able to use AS1 , AS2 and AS3 packaging successfully.

Inbound connection

You can enable your Messenger to receive e-mail messages by setting up a POP/IMAP connection under Configuration → Messenger → eMail 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** – 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



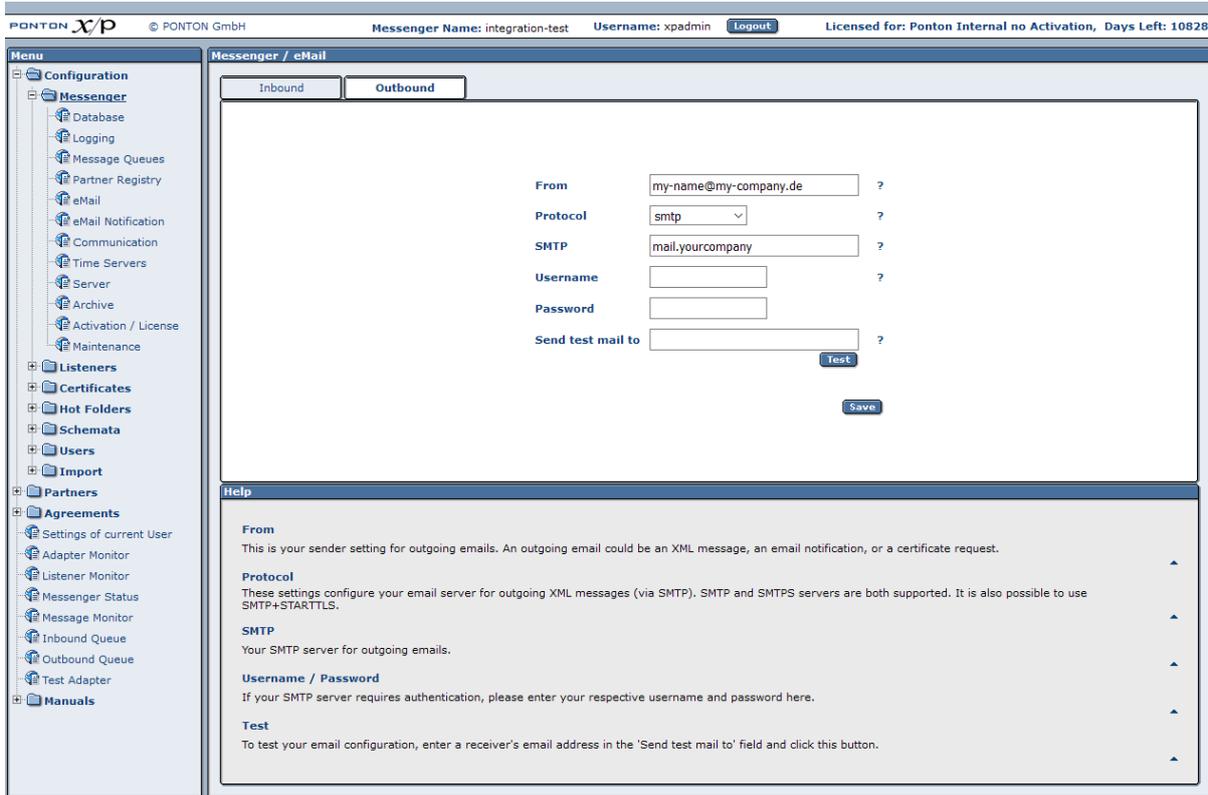
Outbound connection

This connection is used for e-mail messages sent by your Messenger to your business partners. It can be defined under Configuration → Messenger → eMail. The following data needs to be configured:

- **From** – the sender's address to be used for your e-mails
- **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

Test Mail

To test the e-mail connection, enter a receiver e-mail address (in the **Send test mail to** field) and click on **Test**.



The screenshot shows the PONTON X/P Messenger configuration interface. The top bar displays the messenger name 'integration-test', the user 'xpadmin', and a 'Logout' button. The license information is 'Ponton Internal no Activation, Days Left: 10828'. The left sidebar contains a 'Menu' with categories like Configuration, Listeners, Certificates, Hot Folders, Schemata, Users, Import, Partners, Agreements, and Manuals. The main area is titled 'Messenger / eMail' and has tabs for 'Inbound' and 'Outbound'. The 'Outbound' tab is active, showing a configuration form with the following fields:

- From:** my-name@my-company.de
- Protocol:** smtp
- SMTP:** mail.yourcompany
- Username:** (empty)
- Password:** (empty)
- Send test mail to:** (empty)

There are 'Test' and 'Save' buttons at the bottom of the form. Below the form is a 'Help' section with the following text:

From
This is your sender setting for outgoing emails. An outgoing email could be an XML message, an email notification, or a certificate request.

Protocol
These settings configure your email server for outgoing XML messages (via SMTP). SMTP and SMTPS servers are both supported. It is also possible to use SMTP+STARTTLS.

SMTP
Your SMTP server for outgoing emails.

Username / Password
If your SMTP server requires authentication, please enter your respective username and password here.

Test
To test your email configuration, enter a receiver's email address in the 'Send test mail to' field and click this button.

6.1.6. E-mail Notification

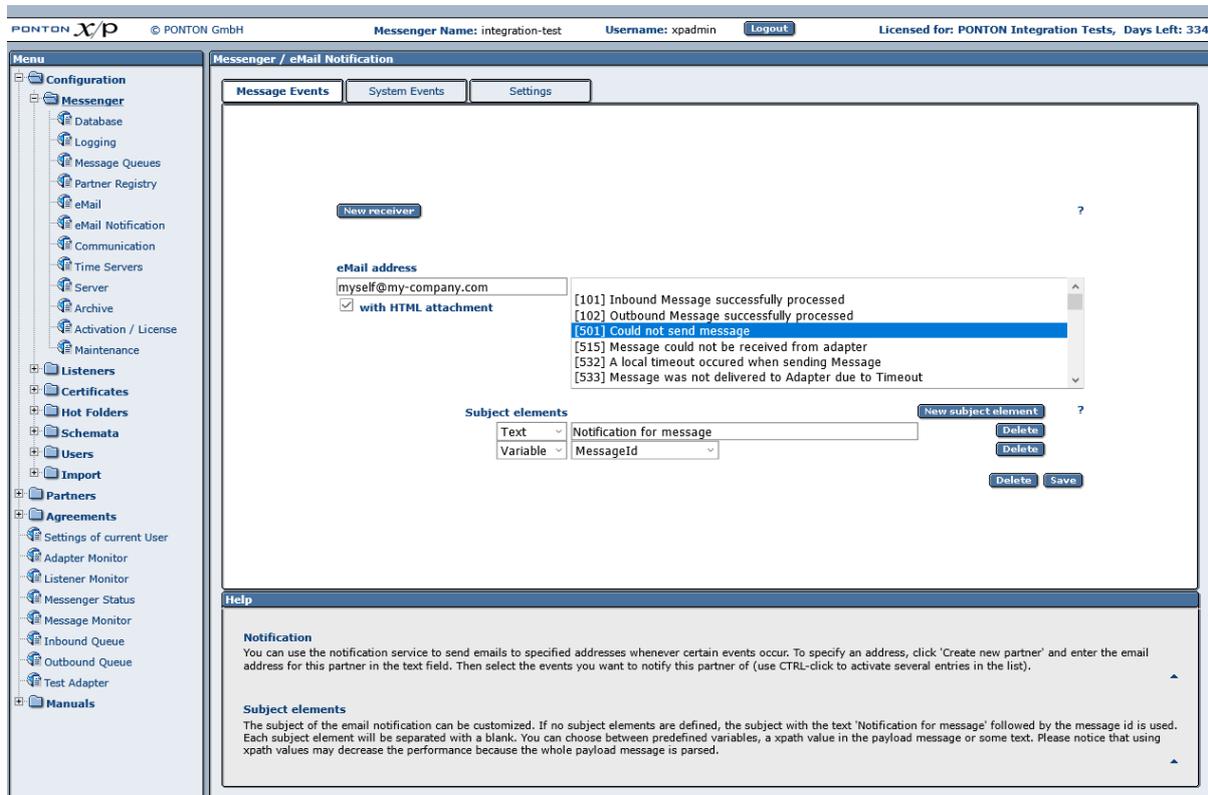
You can use the notification service to send e-mails to specified addresses whenever certain events occur. For example, you might want to notify your system administrator whenever certain errors are encountered. This can be defined under Messenger → eMail Notification. The messenger distinguishes between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

Message Events

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 in the Tab 'Message Events'.

New receiver

To specify an address and event(s) please click **New Receiver**. Enter the e-mail address for this receiver in the text field, and select the events for which this receiver is to be notified. You can use CTRL-click to activate multiple entries in the list.



The screenshot shows the 'Messenger / eMail Notification' configuration window. The 'Message Events' tab is active, displaying a list of events: [101] Inbound Message successfully processed, [102] Outbound Message successfully processed, [501] Could not send message (highlighted), [515] Message could not be received from adapter, [532] A local timeout occurred when sending Message, and [533] Message was not delivered to Adapter due to Timeout. Below the list, the 'Subject elements' section shows two entries: 'Text' with the value 'Notification for message' and 'Variable' with the value 'MessageId'. A 'Help' section at the bottom provides details on the notification service and subject elements.

Subject Elements

If no subject elements are defined, the subject of the e-mail notification will be as follows:
 "Notification for message" + Message ID

By defining one or more subject elements you can customize the subject of the e-mail notification. If you define several subject elements, they will be separated by blanks in the subject line.

For defining subject elements 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 element/value contained in the payload message.

Please note that 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.

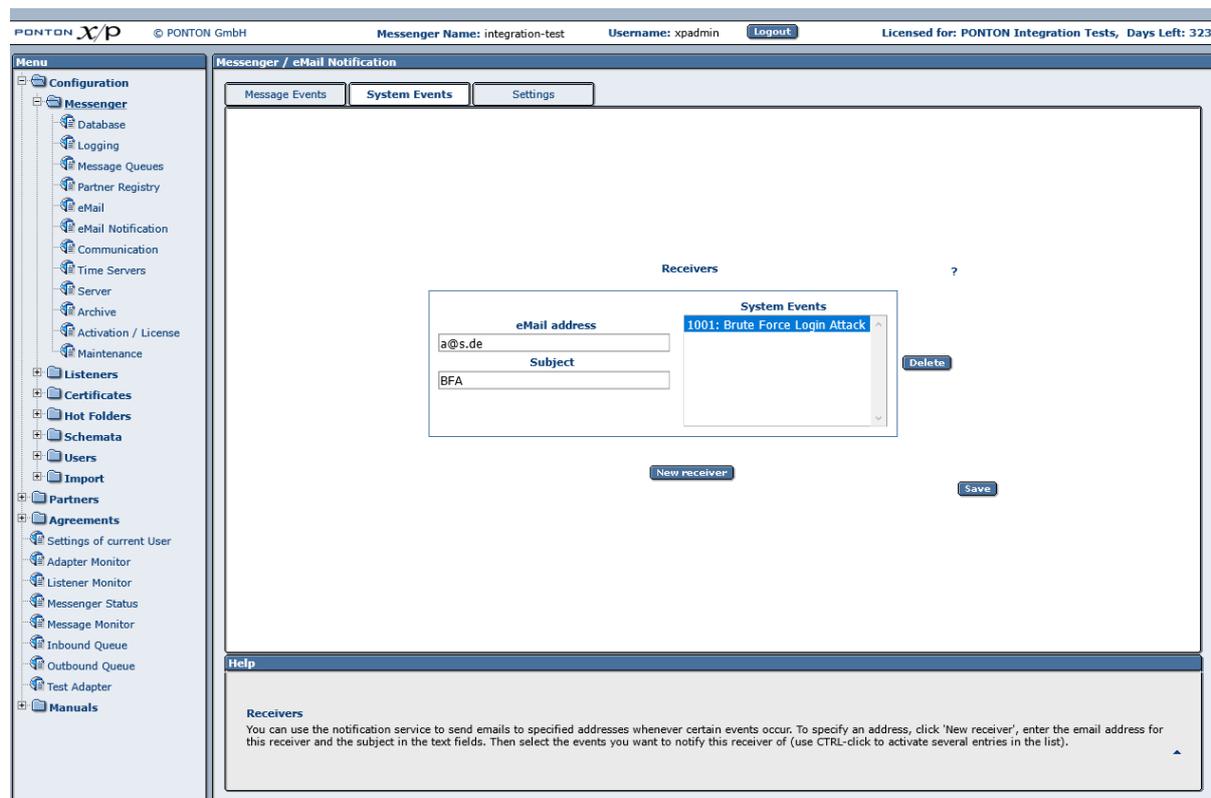
Please note as well that only a subset of the complete xpath syntax is supported for the definition of subject elements. In particular, the following restrictions apply:

- 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.

System Events

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. This can be done in the Tab 'System Events'.



The screenshot shows the PONTON X/P Messenger web interface. The top navigation bar includes the PONTON logo, copyright information (© PONTON GmbH), and user details (Messenger Name: integration-test, Username: xadmin, Logout button, and License information: PONTON Integration Tests, Days Left: 323). The left sidebar contains a 'Menu' with various configuration categories like Configuration, Listeners, Certificates, Hot Folders, Schemata, Users, Import, Partners, and Agreements. The main content area is titled 'Messenger / eMail Notification' and has three tabs: 'Message Events', 'System Events' (which is active), and 'Settings'. The 'System Events' tab displays a 'Receivers' section with a form for adding a new receiver. The form includes an 'eMail address' field (containing 'a@s.de'), a 'Subject' field (containing 'BFA'), and a 'System Events' dropdown menu (showing '1001: Brute Force Login Attack'). There are 'Delete', 'New receiver', and 'Save' buttons. A 'Help' section at the bottom provides instructions: 'You can use the notification service to send emails to specified addresses whenever certain events occur. To specify an address, click 'New receiver', enter the email address for this receiver and the subject in the text fields. Then select the events you want to notify this receiver of (use CTRL-click to activate several entries in the list).'

Settings

To be able to receive mail notifications collectively for multiple events within a time interval the messenger allows you to define cron expressions.

Note: While defining time Intervals for eMail notifications please define the 'Maximum notifications per email' as allowed by your Mailserver.

6.1.7. Communication Settings

On this screen under Configuration → Messenger → Communication you can specify

- **Proxy settings** – if your Messenger will be connecting to the Internet via a proxy server. Please note: The NT Domain is only required if your proxy server uses NTLM authentication.
- If you are going to be using a distributed Listener (as described in the Listener Configuration section) you have the option of also using the Listener as a proxy server for outgoing messages. In this case, click on the **Use Listener Proxy** button to enable use of the Listener as the Messenger's proxy server.
- Retransmission Handling – you can use this setting to specify the number of retransmission attempts and the 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".
- **SSL Server certificate check** – if you enabled this option only communication with Messengers, that use SSL certificates that have been issued by a trusted CA known to your Messenger are allowed.
- **Allow loopback** – makes it possible to send messages from a local partner to another local partner.

There are several tabs under Configuration → Messenger → Communication to configure communication settings for the messenger:

On the **HTTP Proxy** tab you can specify

- **Proxy settings** – if your Messenger will be connecting to the Internet via a proxy server. Please note: The NT Domain is only required if your proxy server uses NTLM authentication.
- If you are going to be using a distributed Listener (as described in the Listener Configuration section) you have the option of also using the Listener as a proxy server for outgoing messages. In this case, click on the **Use Listener Proxy** button to enable use of the Listener as the Messenger's proxy server.
- **Bypass proxy for** – Allows you to define a comma separated list of IPs or fully-qualified hostnames which shall be ignored for the communication via proxy.

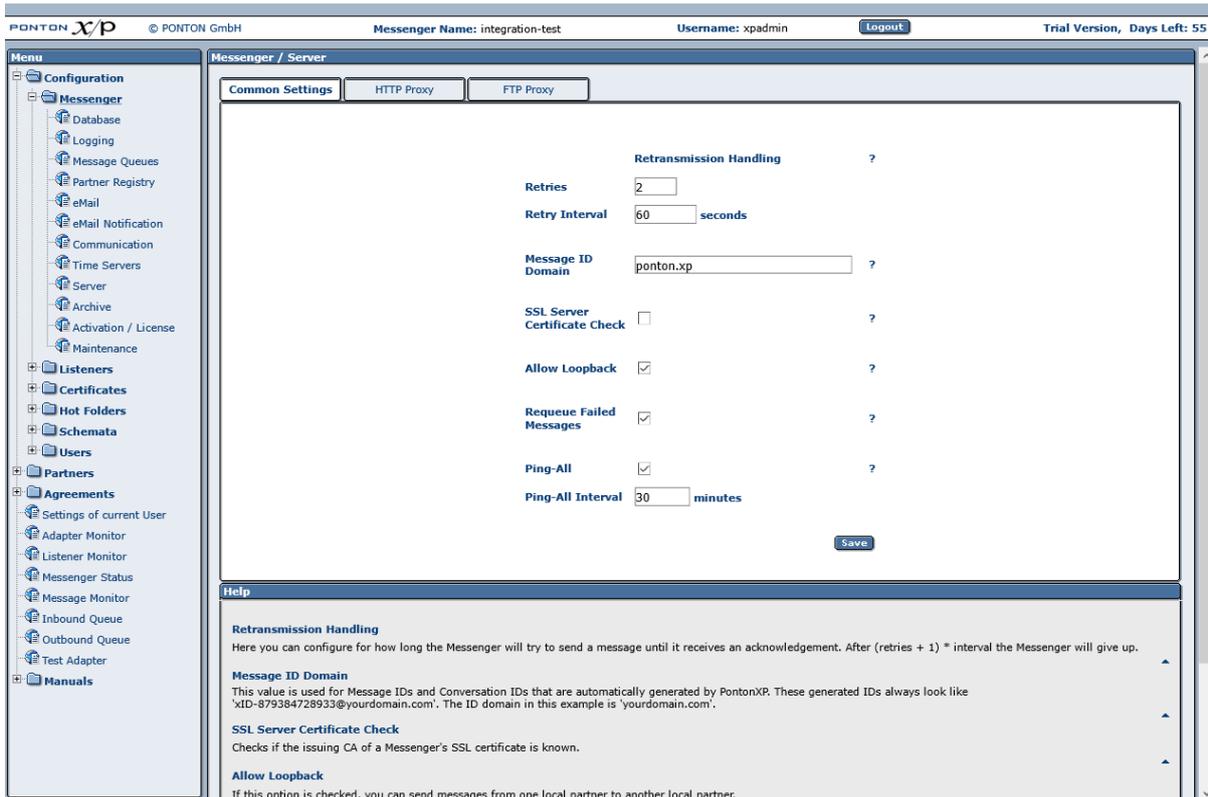
The screenshot shows the X/P Messenger configuration interface. At the top, it displays 'PONTON X/P © PONTON GmbH', 'Messenger Name: integration-test', 'Username: xpadmin', a 'Logout' button, and 'Licensed for: Ponton Internal no Activation, Days Left: 10432'. The left sidebar contains a 'Menu' with categories like Configuration, Messenger, Listeners, Certificates, Hot Folders, Schemata, Users, Import, Partners, Agreements, and Manuals. The main area is titled 'Messenger / Server' and has three tabs: 'HTTP Proxy', 'FTP Proxy', and 'Extended Settings'. The 'HTTP Proxy' tab is active, showing a 'Proxy Configuration' form with fields for IP, Port (set to 3128), Username, Password, and NT Domain. There is also a 'Bypass proxy for' field and a 'Save' button. A 'Use Listener Proxy' button is at the top right of the form. Below the form is a 'Help' section with text explaining proxy configuration and bypassing proxy for specific IPs.

On the **FTP Proxy** tab you can specify a proxy for FTP.

This screenshot shows the same X/P Messenger configuration interface but with the 'FTP Proxy' tab selected. The 'FTP Proxy Configuration' form contains fields for IP, Port, Username, and Password, along with a 'Save' button. The 'Help' section below provides instructions for configuring an FTP proxy, noting that only SOCKS (V4 or V5) proxies can be used.

On the **Common Settings** tab you can specify several additional settings such as

- **Retransmission Handling** – you can use this setting to specify the number of retransmission attempts and the 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 Messengers, that use SSL certificates that have been issued by a trusted CA known to your Messenger are allowed.
- **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.
- **Ping-ALL** - if this option is enabled the Messenger sends ebXML Pings for all agreements with activated Ping-All option and for all defined URLs (primary and fallback) in defined time intervals to check if the communication partner is reachable. 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.



The screenshot shows the 'Messenger / Server' configuration window with the 'Common Settings' tab selected. The 'Retransmission Handling' section contains the following settings:

Setting	Value	Unit
Retries	2	
Retry Interval	60	seconds
Message ID Domain	ponton.xp	
SSL Server Certificate Check	<input type="checkbox"/>	
Allow Loopback	<input checked="" type="checkbox"/>	
Requeue Failed Messages	<input checked="" type="checkbox"/>	
Ping-All	<input checked="" type="checkbox"/>	
Ping-All Interval	30	minutes

Below the settings is a 'Save' button. A 'Help' section at the bottom provides details for each setting:

- Retransmission Handling:** Here you can configure for how long the Messenger will try to send a message until it receives an acknowledgement. After (retries + 1) * interval the Messenger will give up.
- Message ID Domain:** This value is used for Message IDs and Conversation IDs that are automatically generated by PontonXP. These generated IDs always look like 'xID-879384728933@yourdomain.com'. The ID domain in this example is 'yourdomain.com'.
- SSL Server Certificate Check:** Checks if the issuing CA of a Messenger's SSL certificate is known.
- Allow Loopback:** If this option is checked, you can send messages from one local partner to another local partner.

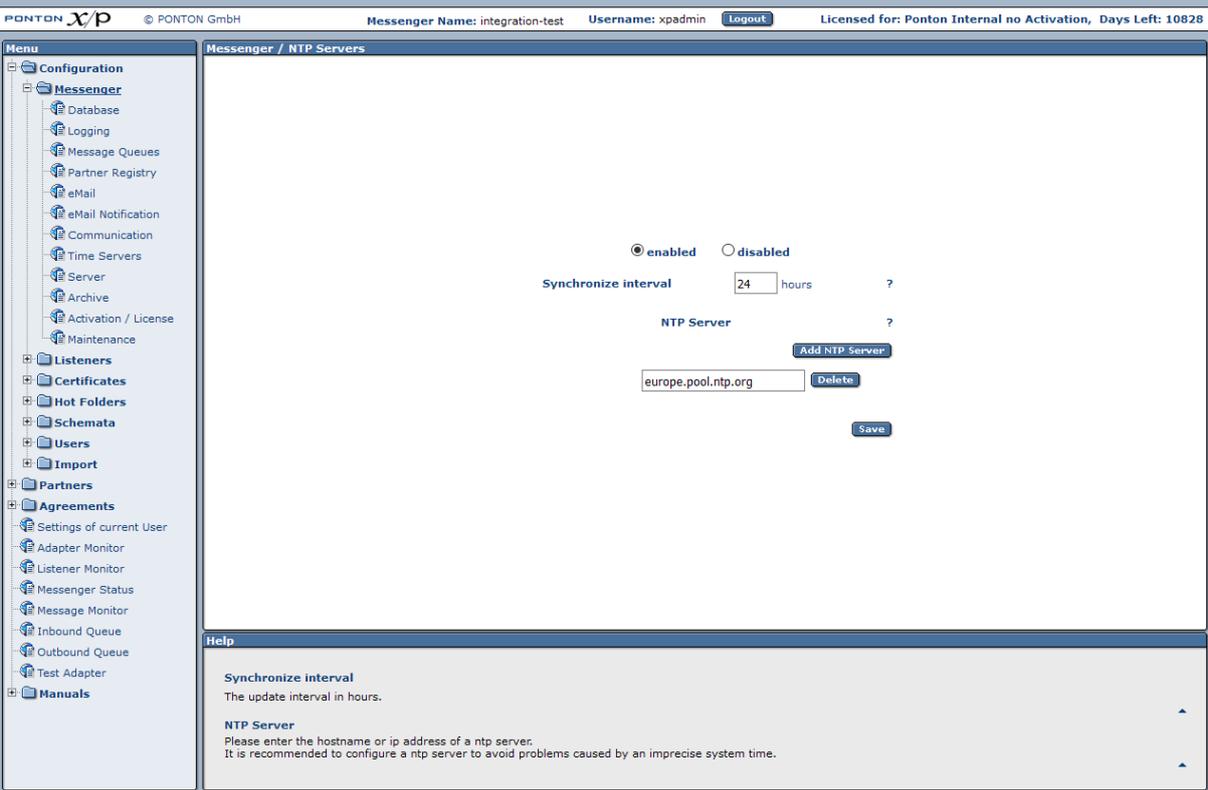
6.1.8. Time Server Configuration

To ensure trouble-free exchange of messages and business transactions, messaging applications like PONTON X/P need to use a correct time setting. 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 the system level, there should be no further need to use additional application level synchronization, since the messenger automatically uses the local systemtime

Viewing or modifying the NTP server configuration can be done in the Messenger Menu: Configuration → Messenger → Time Servers



The screenshot shows the configuration page for NTP Servers. The 'Synchronize interval' is set to 24 hours and is currently enabled. The 'NTP Server' is set to europe.pool.ntp.org. The help section explains that the synchronize interval is the update interval in hours, and an NTP server should be configured to avoid time-related issues.

Depending on your requirements, you can activate/deactivate the Messenger's Time Server synchronization by means of the **enabled/disabled** option. The **Synchronize interval** setting determines how often the application will be synchronized with the NTP server(s) – when enabled. The default setting is to synchronize every 24 hours.

6.1.9. Server configuration

The required ports as well as the SSL certificates for the messenger can be defined in the Messenger Menu: Configuration → Messenger → Server

Connectors

There are different types of connections to the Messenger called Services:

- Listener connections for inbound messages
- Adapter connections for outbound messages
- GUI connection for accessing the web interface

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

You also can change the protocol and the port for the GUI, but please note that only one connector can be defined for the GUI services.

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10828

Menu

- Configuration
 - Messenger
 - Database
 - Logging
 - Message Queues
 - Partner Registry
 - eMail
 - eMail Notification
 - Communication
 - Time Servers
 - Server
 - Archive
 - Activation / License
 - Maintenance
 - Listeners
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Messenger / Server

Connectors SSL Certificate

Connectors ?

Protocol: HTTPS Port: 26843

Services: LISTENERS [Delete] [Create Service]

Protocol: HTTP Port: 26080

Services: GUI [Delete] ADAPTER_SERVICE [Delete] LISTENERS [Delete] [Create Service]

[Create Connector] [Save]

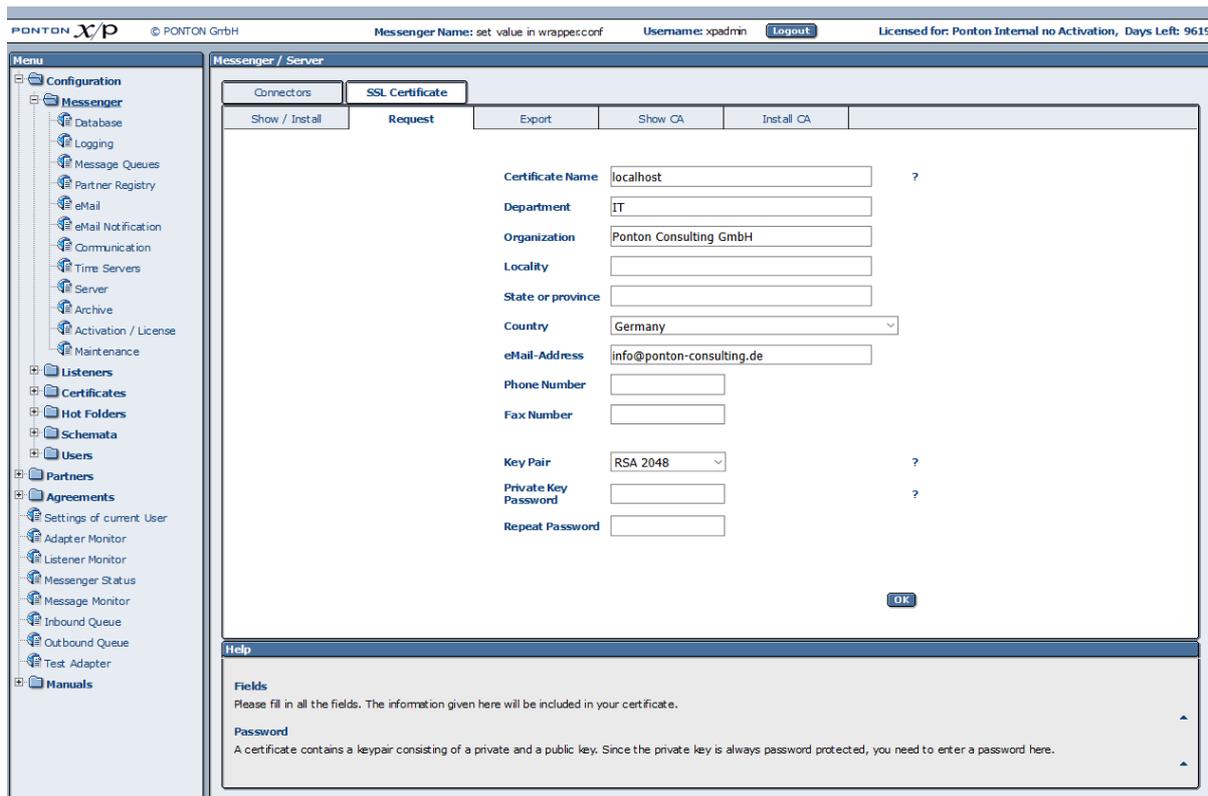
Help

Connectors
 The connector configuration specifies the protocols and ports for the listener, adapter and the GUI services.
 You can create several connectors.
 Note: Only one GUI services can be configured.

SSL-Certificate

This page allows you to request and install a certificate for your server. You need this certificate to be able to receive messages via https. To request a certificate, go to the Request tab and fill in the form – then click **OK**.

While requesting an SSL certificate please mention the Hostname or IP of your messenger machine as the Server-URL. The Hostname or IP should be identical with the Hostname or IP used by your remote partners to connect with your Messenger.



When you receive the SSL certificate, copy and paste it into the text box on the Show/Install tab.

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

SSL cipher and protocol restrictions

HTTPS connectors can be configured to disallow unwanted ciphers and protocol versions.

By default only these protocols are excluded:

- SSL 1.0
- SSL 2.0
- SSL 3.0

These ciphers are excluded by default:

- *EXPORT*
- *anon*
- *DES*
- *_DH*
- *NULL*

- *SHA

The accepted and rejected ciphers are logged at startup in the messenger.log file. This information can also be used to excluded additional unwanted ciphers.

To configure the the excluded ciphers and protocols, please add the elements **ExcludedProtocols** and **ExcludedCiphers** to the SSL element in the server.xml file as shown below:

Code Block 5 server.xml

```

    <SSL>
      <Keystore>$XP_CONFIG_FOLDER/keystore-ssl</Keystore>

      <KeystorePassword>UFhQUFdD9RuIBvTcwnqzDJ0Va6YBBZe7+nw8AvjJdPNjeNRpx3Y=</KeystoreP
      assword>

      <KeyPassword>UFhQUFdDLcckGHm5BlIZP0xprkcsOXx21/nYxjb6tt7/Ek00EBM=</KeyPassword>
      <ClientAuthKeystore>$XP_CONFIG_FOLDER/keystore-
      ssl</ClientAuthKeystore>

      <ClientAuthKeystorePassword>UFhQUFdDYyzC1jdtawW2OU09iYymQnmXGGTNjUUzdukR3mLnkw=<
      /ClientAuthKeystorePassword>
      <ClientAuthentication>none</ClientAuthentication>
      <ExcludedProtocols>SSL*</ExcludedProtocols>

      <ExcludedCiphers>*EXPORT*, *anon*, *DES*, *_DH*, *NULL*, *SHA</ExcludedCiphers>
    </SSL>
  
```

A restart of the Messenger is needed to reinitialise the SSL configuration.

6.1.10. Archive Settings

To define the archive settings please navigate to Configuration → Messenger → Archive in the navigation menu.

The Archive Folder setting can be used to indicate the location of the archiving folders. These can be expressed as

- An absolute path to the required folder.
- A relative path beginning with '\$PONTONXP_HOME' – this placeholder refers to the folder [installation root]\data.

The archiving filter stores the following information in a dedicated directory:

- Backend Envelope

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

Each part is stored in a separate file.

In addition to the main Archive Folder, you can define a separate Archive Failed 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.

The Maximum Age setting specifies how long the files will be archived – expressed in days. Files older than the Maximum age can be deleted from the Filesystem and / or the Database as long as the respective options are activated in the messenger configuration:

- Cleanup Time
 - Delete Database Entries
 - Database Maximum Age
 - Delete in File system
 - Maximum File Age

Deletion of files from the file system and / or the database will start at the specified Cleanup Time. If no value for the Cleanup Time is set and cleanup is activated the messenger will automatically start the cleanup at 03:00:00 Hours.

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10828

Menu

- Configuration
 - Messenger
 - Database
 - Logging
 - Message Queues
 - Partner Registry
 - eMail
 - eMail Notification
 - Communication
 - Time Servers
 - Server
 - Archive
 - Activation / License
 - Maintenance
 - Listeners
 - Certificates
 - Hot Folders
 - Schema
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Messenger / Archive

Archive Folder ?

Archive Folder

Archive Failed Folder

use Zip compression

Archivable Message parts ?

Backend Envelope

ebXML

Payload

Certificate

Signature

Attachment

Archive Database and Filesystem?

Cleanup Time

Database Maximum Age days

Delete Database entries

File Maximum Age days

Delete in Filesystem

Help

Archive Folder
 You can specify the archive folder as

- Absolute pathname to the required folder
- Relative pathname beginning with '\$PONTON_XP' - this placeholder refers to the Messenger's 'ebXMLpipe' folder.

Optional Zip compression reduces the size of the Archive on disk.

6.1.11. Activation / License Configuration

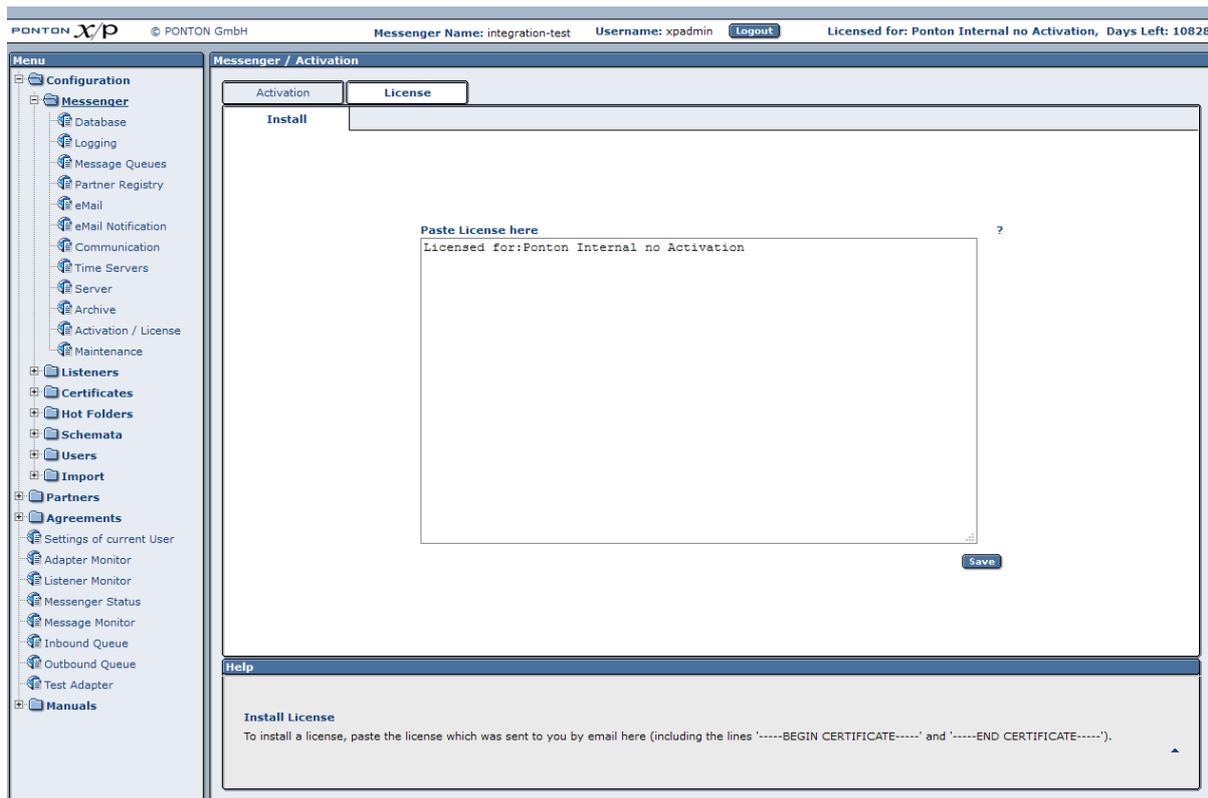
This section describes how to install and activate licenses for Ponton X/P. If you want to activate the software as a trial version, please see the description starting on page .

Installing a license

You will generally receive your Ponton X/P license as a text or e-mail from Ponton or from your licensing organization.

To install your license go to Configuration → Messenger → Activation / License and click on the License tab. Copy the complete license text (including the lines ----BEGIN LICENSE---- and ----END LICENSE----) and paste the license text into the text box on the Install tab.

Click on Save to complete the installation of the license. You should see a message indicating that the license was successfully installed.



Activating an installed license

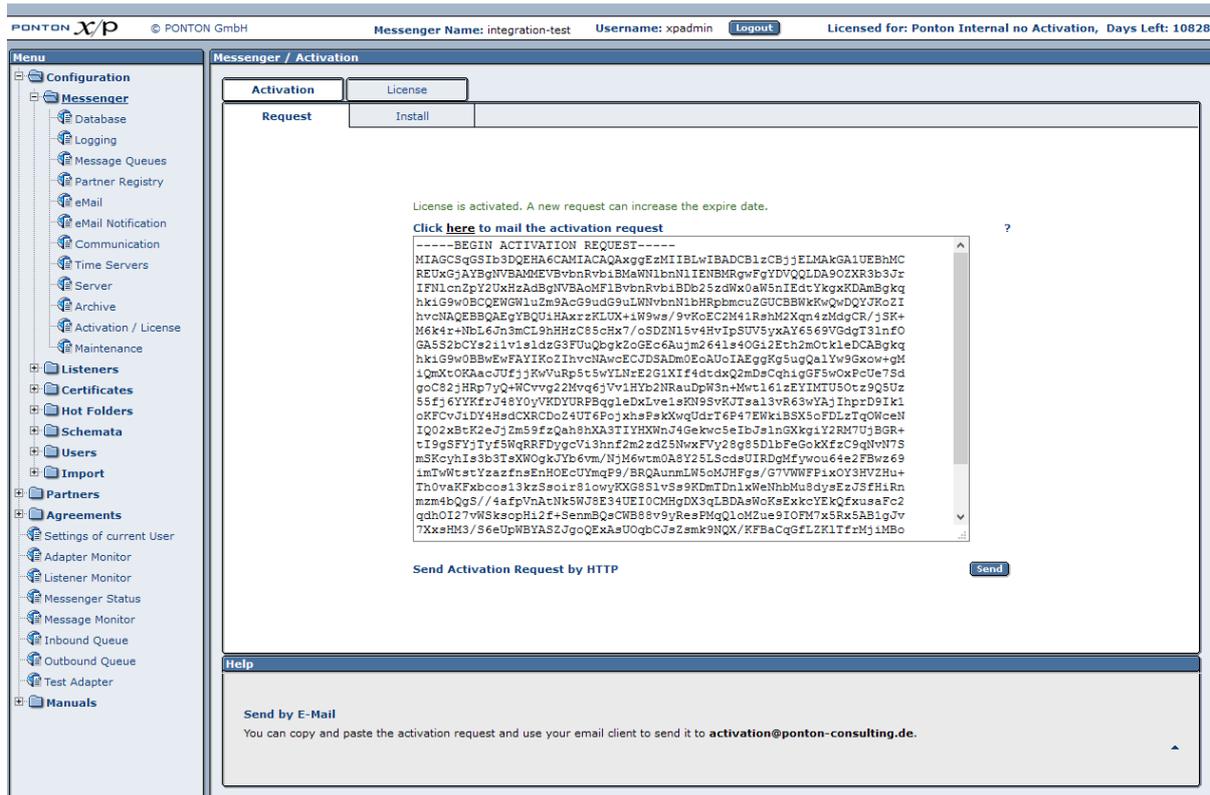
Depending on your license conditions it may be necessary to activate your license after it is installed. If so, you will see a Create Activation link in the upper right corner and on the Messenger Status screen.

Requesting a license activation

To activate your license go to Configuration → Messenger → Activation / License and click on the Activation Request tab or simply click the Create Activation link. This will call up the Activation Request tab with a box containing your activation request.

The easiest and fastest way to complete your license activation is to click on the **Send** button (below the text box on the Activation Request tab). This will activate the license almost immediately. You should see a message indicating that *your license was successfully activated*.

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.



To submit your activation request by e-mail, as with the trial version (see page), click on the **e-mail** link at the top of the Activation Request tab or copy the complete activation request and send it to activation@ponton.de using your preferred e-mail client.

Notes

- 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 -----". This is also the case when copying the activation code from the reply e-mail into the Install tab. Again, please be sure to include the "Begin" and "End" lines.
- Depending on your license conditions, you may need to *repeat the license activation process* after making certain changes to your local partner configuration. In that case, the you will a red text in the upper right corner of your messenger screen requesting you to **'Create Activation'**

Installing a license activation

If you have submitted a license activation request via eMail you will receive a reply containing your activation code, which you can then copy and paste into the text box on the Install tab. Then click the **Save** button to complete your license activation. Following the activation the message in the upper right corner and the Messenger Status screen will indicate the name and the remaining lifetime of the license, for example:

Licensed for: PONTON GmbH, Days left: 1096

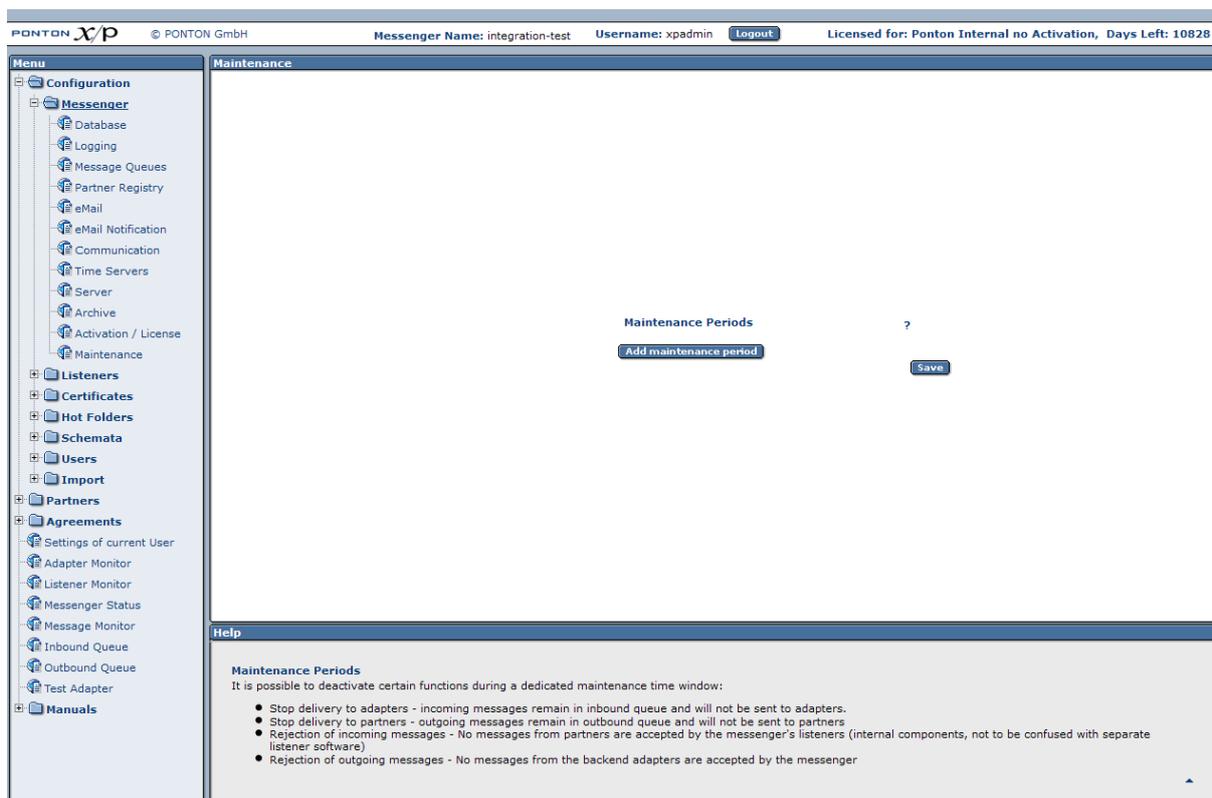
6.1.12. Maintenance

Maintenance is used to disable the follow services:

- *Stop delivery to adapters* - incoming messages remain in inbound queue and will not be sent to adapters.
- *Stop delivery to partners* - outgoing messages remain in outbound queue and will not be sent to partners
- *Rejection of incoming messages* - No messages from partners are accepted by the messenger's listeners (internal components, not to be confused with separate listener software)
- *Rejection of outgoing messages* - No messages from the backend adapters are accepted by the messenger

To enable maintenance, at least one maintenance period must be created. During this time the Messenger the selected services will not be active.

Maintenance periods can be defined under Configuration → Messenger → Maintenance :



The screenshot shows the PONTON X/P Messenger web interface. The top navigation bar includes the PONTON logo, version information, and user details. The left sidebar contains a menu with categories like Configuration, Listeners, Certificates, and Partners. The main content area is titled 'Maintenance' and displays 'Maintenance Periods' with a question mark icon. Below this, there are two buttons: 'Add maintenance period' and 'Save'. A 'Help' section at the bottom provides a definition of maintenance periods and a list of services that can be deactivated during this time.

Maintenance Periods ?

[Add maintenance period](#) [Save](#)

Help

Maintenance Periods
 It is possible to deactivate certain functions during a dedicated maintenance time window:

- Stop delivery to adapters - incoming messages remain in inbound queue and will not be sent to adapters.
- Stop delivery to partners - outgoing messages remain in outbound queue and will not be sent to partners
- Rejection of incoming messages - No messages from partners are accepted by the messenger's listeners (internal components, not to be confused with separate listener software).
- Rejection of outgoing messages - No messages from the backend adapters are accepted by the messenger

6.2. Listener Settings

The settings in this section are used to specify the Listener configuration in a distributed installation. For details please refer to the section 'Listener Configuration' in the chapter 'Advanced Configuration'.

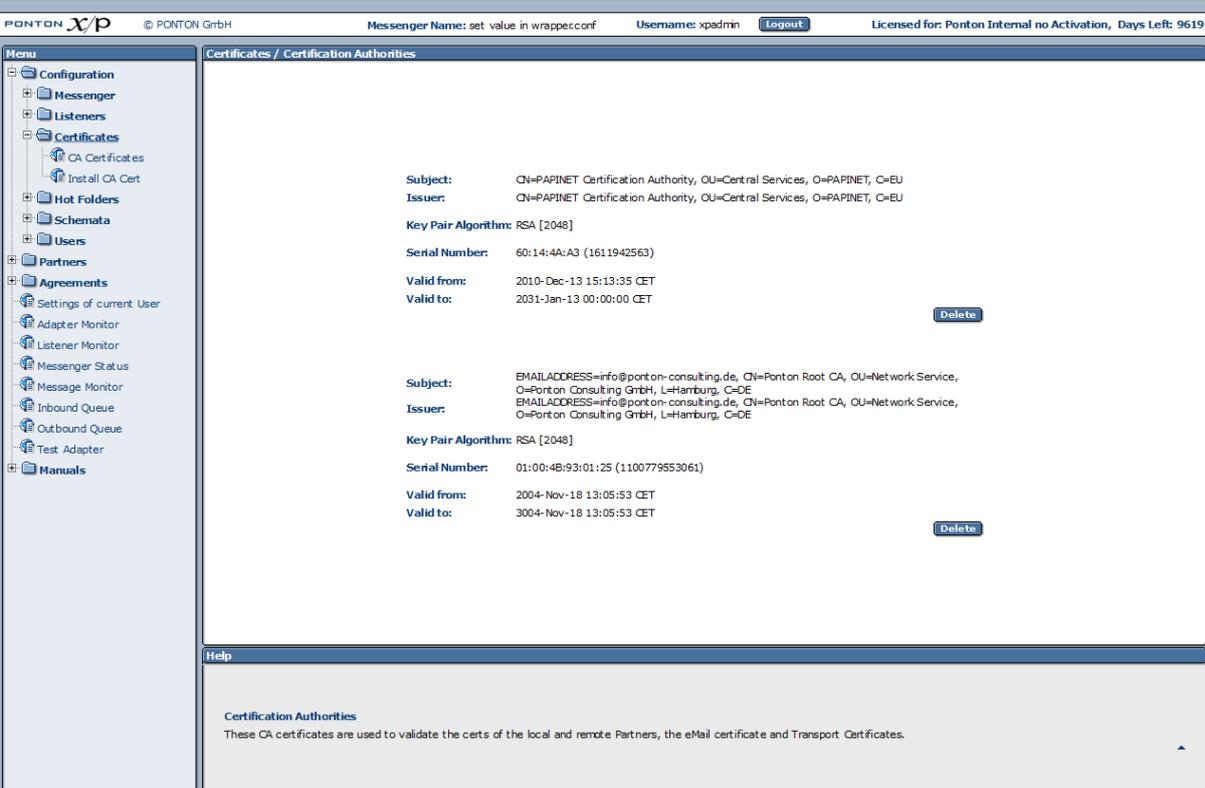
6.3. CA Certificates

PONTON X/P uses trusted certificates to ensure the identity and authorization of partner configurations. PONTON offers its own lightweight certification authority, which can be used in connection with PONTON X/P messaging. This is the default CA in a standard PONTON X/P installation and the PONTON CA certificate is automatically installed with the software.

If you want to use certificates issued by a 3rd party CA you will need to request and install the root certificate of the CA. You will not be able to install partner certificates issued by a given CA until the CA's root certificate has been installed.

When you receive the CA's root certificate go to Configuration → Certificates → Install CA Cert and then copy and paste the certificate into the text field. If you received the CA certificate as a file (e.g. *.cer) you can use the Browse function to select the file for import. Click Save to add this CA certificate to your Messenger configuration.

To show the currently installed CA Certificates select Configuration → Certificates → CA Certificates:



The screenshot shows the PONTON X/P web interface. The top navigation bar includes the PONTON logo, copyright information (© PONTON GmbH), Messenger Name (set value in wrapper.conf), Username (xadmin), a Logout button, and license information (Licensed for Ponton Internal no Activation, Days Left: 9619).

The left sidebar contains a 'Menu' with the following items: Configuration, Messengers, Listeners, Certificates (expanded to show CA Certificates and Install CA Cert), Hot Folders, Schemata, Users, Partners, Agreements, Settings of current User, Adapter Monitor, Listener Monitor, Messenger Status, Message Monitor, Inbound Queue, Outbound Queue, Test Adapter, and Manuals.

The main content area is titled 'Certificates / Certification Authorities' and displays two certificates:

- Certificate 1:**
 - Subject: CN=PAPINET Certification Authority, OU=Central Services, O=PAPINET, C=EU
 - Issuer: CN=PAPINET Certification Authority, OU=Central Services, O=PAPINET, C=EU
 - Key Pair Algorithm: RSA [2048]
 - Serial Number: 60:14:4A:A3 (1611942563)
 - Valid from: 2010-Dec-13 15:13:35 CET
 - Valid to: 2031-Jan-13 00:00:00 CET
 - Delete button
- Certificate 2:**
 - Subject: EMAILADDRESS=info@ponton-consulting.de, O=Pont on Root CA, OU=Network Service, O=Pont on Consulting GmbH, L=Hamburg, C=DE
 - Issuer: EMAILADDRESS=info@ponton-consulting.de, CN=Pont on Root CA, OU=Network Service, O=Pont on Consulting GmbH, L=Hamburg, C=DE
 - Key Pair Algorithm: RSA [2048]
 - Serial Number: 01:00:4B:93:01:25 (1100779553061)
 - Valid from: 2004-Nov-18 13:05:53 CET
 - Valid to: 3004-Nov-18 13:05:53 CET
 - Delete button

At the bottom, there is a 'Help' section titled 'Certification Authorities' with the text: 'These CA certificates are used to validate the certs of the local and remote Partners, the eMail certificate and Transport Certificates.'

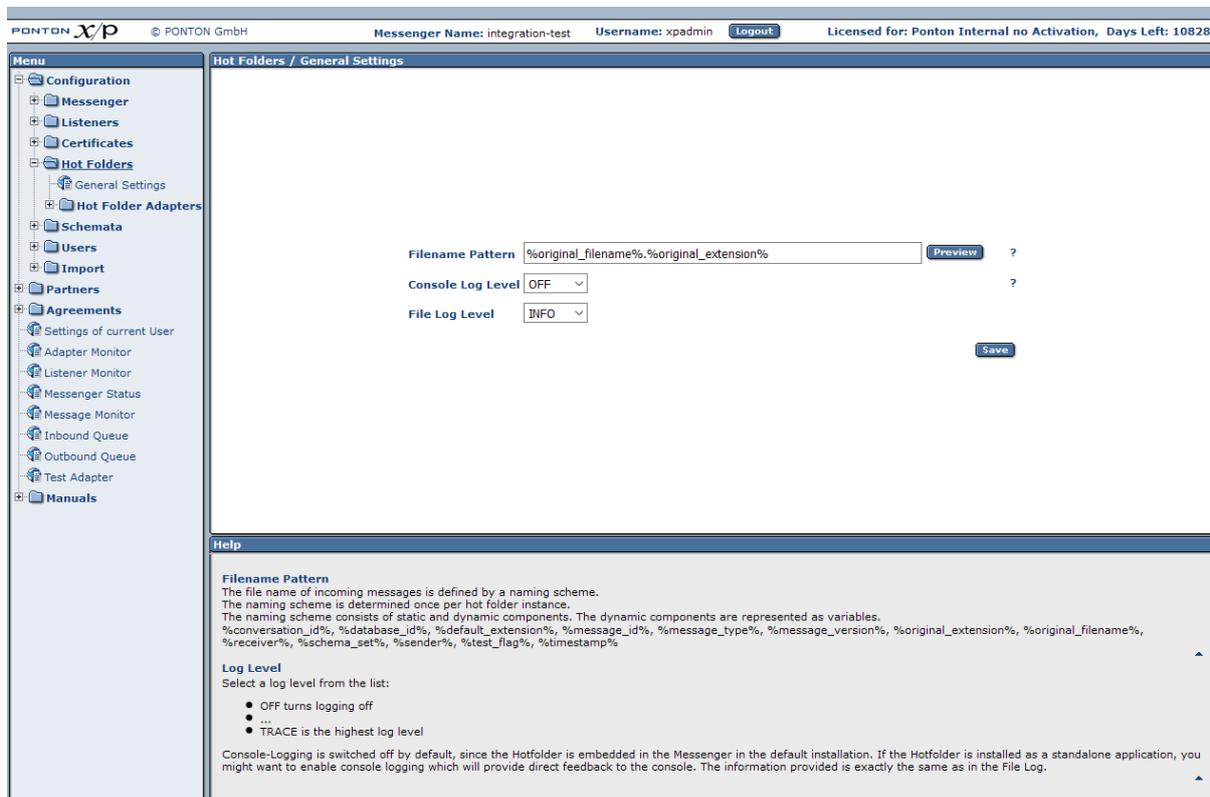
6.4. Hot Folder Adapter (HFA)

To set up a hotfolder adapter to send and / or receive files please navigate to Configuration → Hot Folders in the messenger menu.

6.4.1. General Configuration

To define the following globally common values for all hot folder adapters please navigate to Configuration → Hot Folders → General Settings:

Filename Pattern – this property defines a pattern for filenames to be used while saving incoming files in an HFA. This general property allows the user to define a filename pattern to be used by every newly created hot folder as long as no other filename pattern is defined for the individual hot folder.



The screenshot shows the X/P Messenger web interface. The top navigation bar includes the PONTON logo, copyright information, Messenger Name (integration-test), Username (xpadmin), a Logout button, and license information (Ponton Internal no Activation, Days Left: 10828). The left sidebar menu is expanded to 'Hot Folders / General Settings'. The main content area contains the following configuration options:

- Filename Pattern:** A text input field containing the pattern `%original_filename%.%original_extension%`, with a 'Preview' button and a help icon.
- Console Log Level:** A dropdown menu set to 'OFF'.
- File Log Level:** A dropdown menu set to 'INFO'.
- A 'Save' button is located at the bottom right of the configuration area.

The bottom section of the page is a 'Help' panel with the following content:

Filename Pattern
 The file name of incoming messages is defined by a naming scheme. The naming scheme is determined once per hot folder instance. The naming scheme consists of static and dynamic components. The dynamic components are represented as variables.
`%conversation_id%, %database_id%, %default_extension%, %message_id%, %message_type%, %message_version%, %original_extension%, %original_filename%, %receiver%, %schema_set%, %sender%, %test_flag%, %timestamp%`

Log Level
 Select a log level from the list:

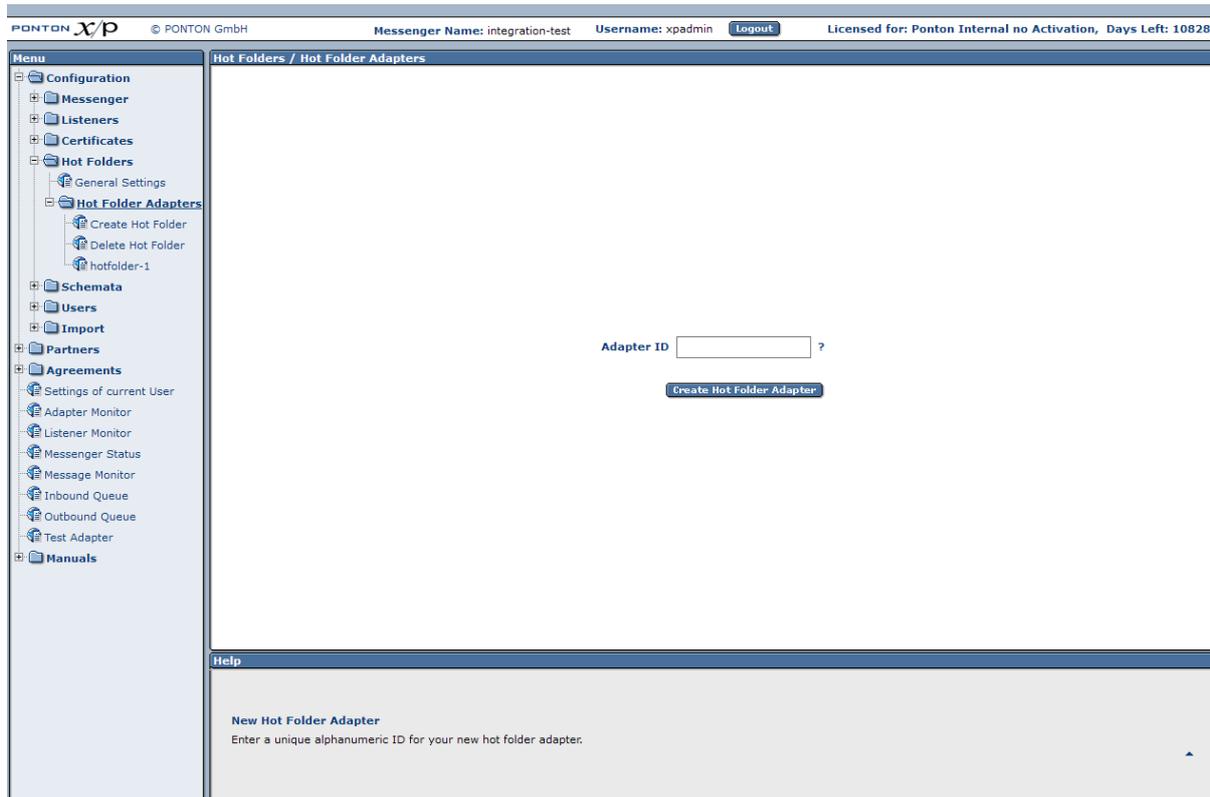
- OFF turns logging off
- ...
- TRACE is the highest log level

Console-Logging is switched off by default, since the HotFolder is embedded in the Messenger in the default installation. If the HotFolder is installed as a standalone application, you might want to enable console logging which will provide direct feedback to the console. The information provided is exactly the same as in the File Log.

6.4.2. Create / Delete Hot Folder

The messenger allows you to configure more than one Hot Folder Adapter simultaneously. The HFAs are created and deleted on the respective configuration pages under Configuration → Hot Folder Adapters → Create Hot Folder (or Delete Hot Folder). Each HFA registers under a different ID with the Messenger. HFAs may be created for

individual partners – in this case, messages exchanged with other partners will be stored and processed by means of the default HFA.



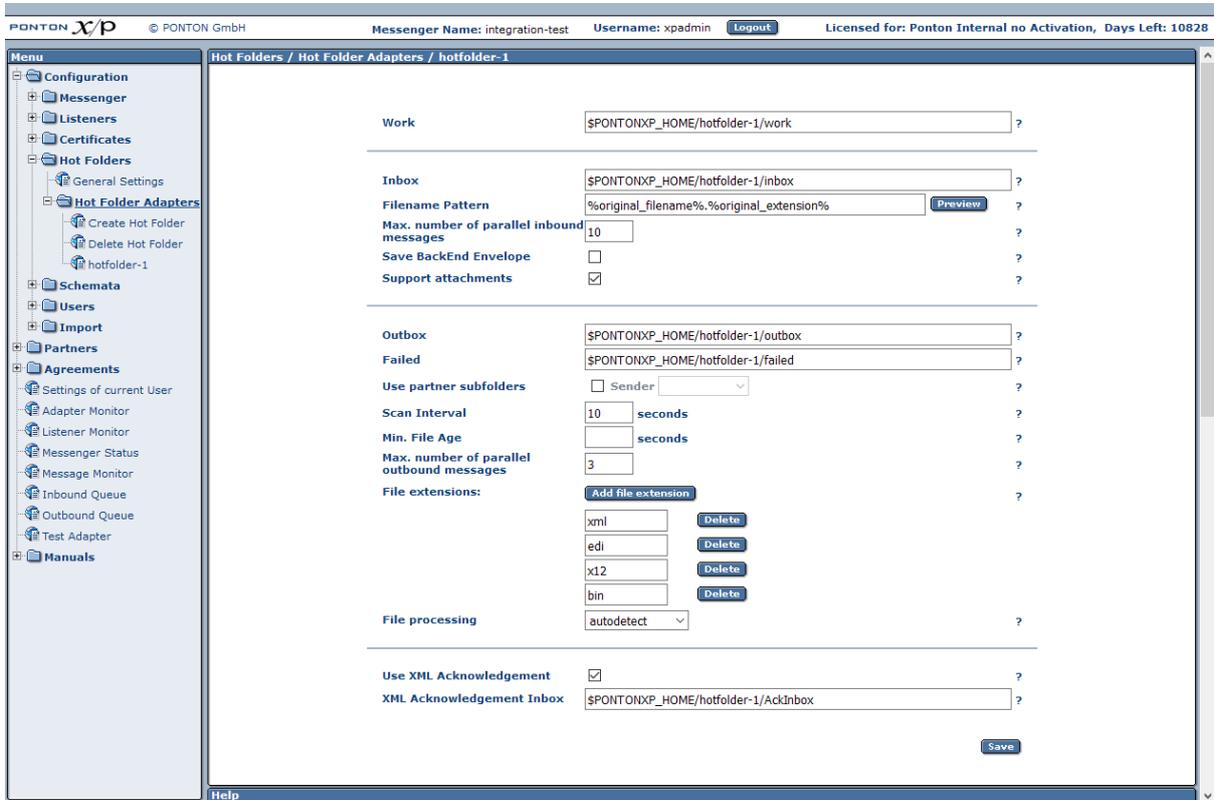
6.4.3. Configuring an Hot Folder Adapter

To define the specific settings for each one of your hot folder adapters please navigate to Configuration → Hot Folders → Hot Folder Adapters → <Your Hotfolder, such as hotfolder-1>.

Each HFA requires several directories to be defined. These directories are created by the HFA if they do not already exist:

- Work – this folder temporarily contains document related data while documents are being processed by the messenger. This data is removed as soon as the document is successfully processed and completely stored in the folder.
- Inbox – this folder stores incoming documents whenever received from a partner.
- Outbox – documents to be sent to the business partner are dropped into the Outbox folder. Every Scan Interval the messenger processes the files lying in the Outbox folder(s).
- Failed – if a document cannot be sent successfully to a partner due to a local messenger error, it will be stored in this folder. For eg. if the xml file to be sent is not valid according to schema.

- Inbox for XML acknowledgements – the HFA can save technical acknowledgements (ACK messages) if required for the the backend ERP application. These ACK messages are saved in a separate Inbox than the incoming messages and is also known as **AckInbox**



PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10828

Menu
 Configuration
 Messenger
 Listeners
 Certificates
 Hot Folders
 General Settings
Hot Folder Adapters
 Create Hot Folder
 Delete Hot Folder
 hotfolder-1
 Schemata
 Users
 Import
 Partners
 Agreements
 Settings of current User
 Adapter Monitor
 Listener Monitor
 Messenger Status
 Message Monitor
 Inbound Queue
 Outbound Queue
 Test Adapter
 Manuals

Hot Folders / Hot Folder Adapters / hotfolder-1

Work: \$PONTONXP_HOME/hotfolder-1/work ?

Inbox: \$PONTONXP_HOME/hotfolder-1/inbox ?

Filename Pattern: %original_filename%.%original_extension% Preview ?

Max. number of parallel inbound messages: 10 ?

Save BackEnd Envelope: ?

Support attachments: ?

Outbox: \$PONTONXP_HOME/hotfolder-1/outbox ?

Failed: \$PONTONXP_HOME/hotfolder-1/failed ?

Use partner subfolders: Sender: ?

Scan Interval: 10 seconds ?

Min. File Age: seconds ?

Max. number of parallel outbound messages: 3 ?

File extensions: Add file extension ?

xml Delete
 edi Delete
 x12 Delete
 bin Delete

File processing: autodetect ?

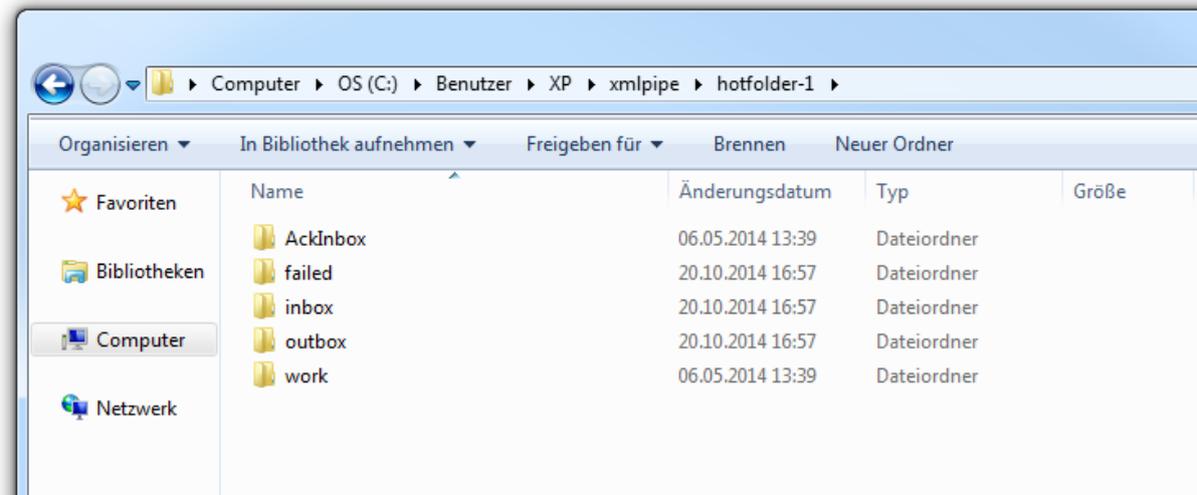
Use XML Acknowledgement: ?

XML Acknowledgement Inbox: \$PONTONXP_HOME/hotfolder-1/AckInbox ?

Save

Work, Outbox and Failed folders are created automatically on the filesystem while creating a new HFA. Inbox & AckInbox folders are only created once incoming messages and ACKs are received.

The HFA folder structure looks like this in the filesystem:



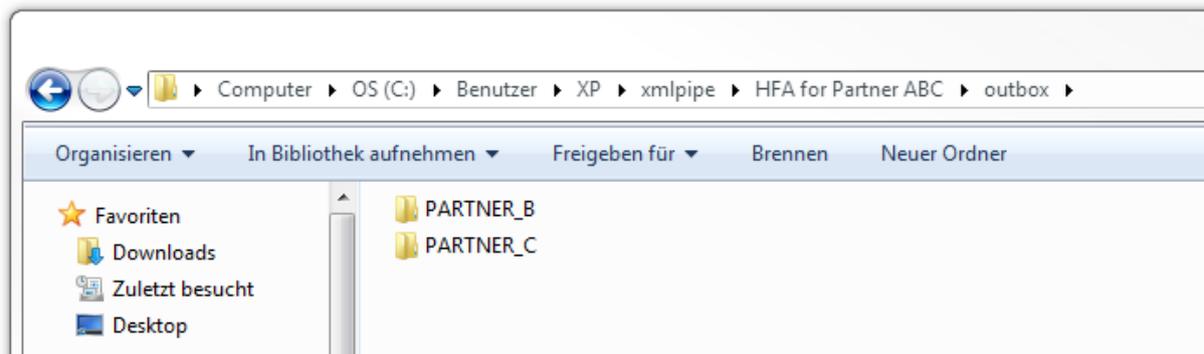
Further settings supported by the hot folder adapter are listed here :

- Port – this property is optional. This defines the port to be used by the HFA.
- Filename pattern – this property defines the filename pattern of files to be saved in the Inbox folder of this HFA. Only pre-defined variables can be used for the configuration of filename patterns which are defined in the section 'Filename patterns' below.
- Max. number of parallel inbound messages – specifies the maximum number of receiving threads the adapter can process simultaneously.
- Save Backend envelope – allows the backend envelope of the incoming messages to be retained
- Support attachments – the HFA will save files attached to an incoming message to the selected inbox folder
- Use partner subfolders – if this is set, this HFA will create partner subfolders in it's own outbox folder with valid communication partners. The subfolder function is described in the section 'Subfolder function' below.
- Scan Interval – the interval to wait (in seconds) between checking the outbox
- Minimum File age - the minimum file age (in seconds) to process any file. If this value is set, the hotfolder will skip all files with modification date not older than the defined min. file age.
- Max. number of parallel outbound messages – specifies the maximum number of sending threads the adapter can process simultaneously.
- File extension – only files with extensions specified here will be collected and processed by the HFA from the outbox folder. The supported extensions can be adjusted according to the needs of the backend (ERP) applications.
- File processing – this value specifies the expected content of the files lying in the outbox of the particular HFA regardless of the file extensions. This functionality is described in the section ' Processing options' below.

- Use XML acknowledgement – with this option activated, the HFA can save technical acknowledgements (ACK messages) in the AckInbox folder sent by the communication partner upon receiving the messages sent from your side.

Subfolder function

By activating the 'Use Partner Subfolder' option for a local Partner (such as PARTNER_D) as the standard Sender of messages in the HFA configuration subfolders will automatically be created in the outbox:



The subfolders in the outbox are only created for Partners with a valid agreement with PARTNER_D :

		Outbound							Inbound		
Partner 1	Partner 2	Protocol	Packaging	Pipeline	Adapter	Packaging	Pipeline				
PARTNER_C	PARTNER_D	HTTP	EbXml20	Messenger 2.1	EdaAdapter	EbXml20	Messenger 2.1				
PARTNER_D	PARTNER_B	HTTP	EbXml20	Messenger 2.1	TEST-HF	EbXml20	Messenger 2.1				
PARTNER_C	PARTNER_B	HTTP	EbXml20	Messenger 2.1	TEST-GB	EbXml20	Messenger 2.1				
PARTNER_C	EDATEST	HTTPS	EbXml20	Messenger 2.1	TEST-HF	EbXml20	Messenger 2.1				

The Hot-Folder-Adapter searches for and processes files from all subfolders on the filesystem underneath the configured Outbox path. In case more than just the valid partner-subfolders exist (manually or automatically) within the configured Outbox, please be aware that the hotfolder will try to process the files within these invalid subfolders and move these file to another location (into the configured Failed folder) after that.

Filename Patterns

Following parameter values are supported as Filename patterns in the enhanced Hot Folder:

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.
%conversation_id%	Text	Message ID as defined by the sender.
%sender%	Text	Internal Partner-ID of the sender in the local messenger.

Variable	Type	Description of this value
%receiver%	Text	Internal Partner-ID of the receiver in the local messenger.
%message_type%	Text	Message Type as recognised by the messenger. This depends on the activated SchemaSet as well as the agreement configuration in the messenger.
%schema_set%	Text	Schemaset as defined in the messenger for the agreement between these particular partners.
%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 original Filename without extension as sent by the sender of this message.
%default_extension%	Text	Standard-File-Extension for the received Filecontent.
%original_extension%	Text	Original extension as sent by the sender of this message.

These parameter values can also be used to be define folder paths and/or filenames individually for the following items in the Hot Folder Configuration:

- Inbox
- Filename Pattern
- AckInbox

A list of widely used combinations of these values can be seen in the table below:

Example: Filename pattern configured in the messenger	Example: Result of the filename on the filesystem	Hint
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 messagetype and schemaset
%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

Example: Filename pattern configured in the messenger	Example: Result of the filename on the filesystem	Hint
		the time of saving the file on the filesystem as variant time .

Inbox Patterns

As mentioned variables can also be used to define (Ack-)Inbox-paths. The following example 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	<ul style="list-style-type: none"> • This folder will only be created once an incoming message has been received by the hot folder • %sender% describes the sender of the incoming message • %receiver% describes the receiver of the incoming message

Processing options

Processing options help to define the content of the files which are dropped into the hotfolder outbox irrespective of their file extensions. The following table elaborates on the use of these processing options:

File Extension	Processing option	processing description
<ul style="list-style-type: none"> • txt • edi • xml • x12 	autodetect	Using this configuration of the Hot Folder following result can be expected: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ○ as an XML message <ul style="list-style-type: none"> ▪ if the content of the 'xml' file can be recognised as a valid XML ▪ and if XML is activated in the Schemaset of the

File Extension	Processing option	processing description
		<p style="text-align: center;">Agreement</p> <ul style="list-style-type: none"> ○ as a BINARY message <ul style="list-style-type: none"> ▪ if the file has the extension 'txt' ▪ and if BINARY is activated in the Schemaset of the Agreement <p style="text-align: center;">Hint: All formats other than 'xml', 'x12' and 'edi' will be processed as BINARY as long as-autodetect is activated</p>
<ul style="list-style-type: none"> • txt • edi • xml • x12 • png • pdf 	Binary	<p>Using this configuration of the Hot Folder following result can be expected:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ BINARY is activated in the Schemaset of the Agreement

6.5. Global Schema Configuration

The schema sets to be supported for each partner are defined in the partner configuration. The standard schema sets available within the messenger are shown under Configuration → Schemata:

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10834

Menu

- Configuration
 - Messenger
 - Listeners
 - Certificates
 - Hot Folders
 - Schemata
 - Schema Set Upload
 - BINARY
 - consumption01.01
 - ebUtilities1.11
 - ebUtilities2.00
 - EDIFACT_D99A
 - papinet2.40 (20080508)
 - wp1.0
 - wp2.01
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Schemata / ebUtilities1.11

Schema Set ebUtilities1.11
 Schema Folder ebutilities1.11
 XSL Folder ebutilities1.11

Type	Version	Location	XSL	Namespace
Invoice	V1R11	http://www.ebutilities.at/invoice/01p11	✓	http://www.ebutilities.at/invoice/01p11
Cancellation	V1R11	http://www.ebutilities.at/cancellation/01p11	✓	http://www.ebutilities.at/invoice/01p11

6.5.1. Adding a new SchemaSet

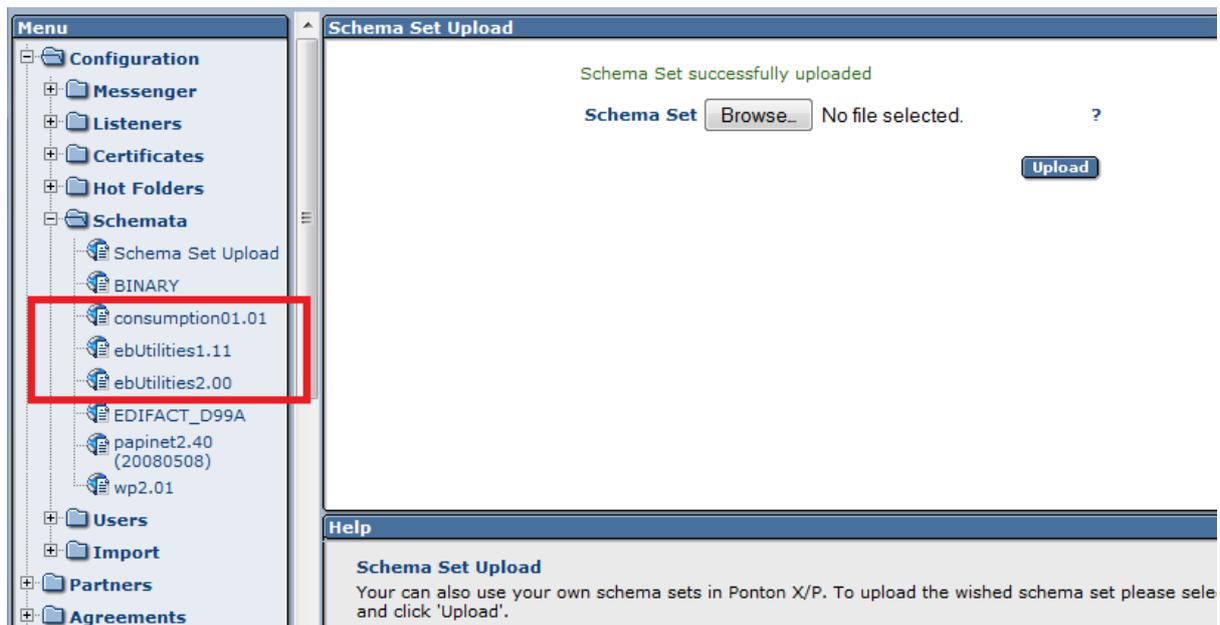
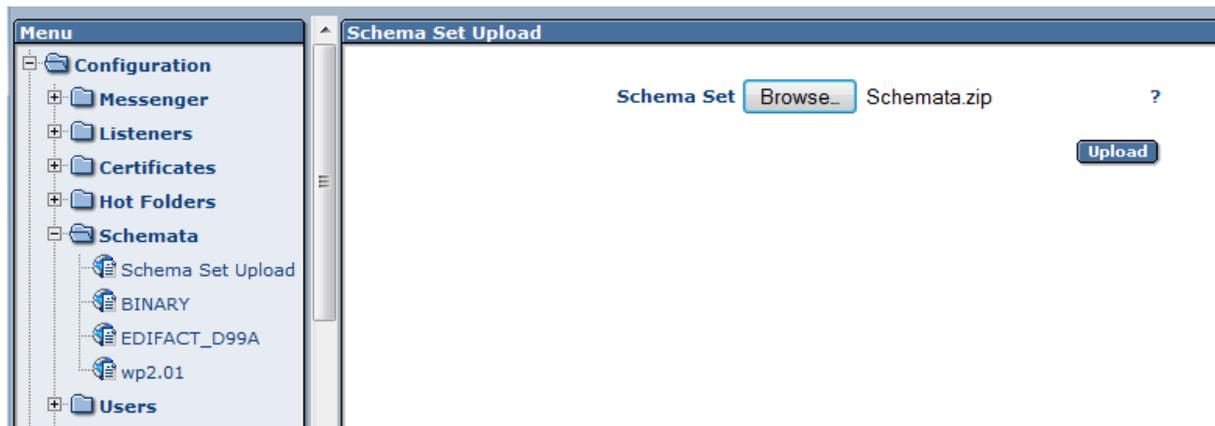
To add a new SchemaSet to the messenger you require an .xsd as well as an .xml which define this SchemaSet. There are different methods which allow you to define new SchemaSets in the messenger.

Configuration enhancement

By including the SchemaSet .xsd as well as .xml file to the configuration folder of the messenger. This method is described in the section 'Adding a new Schema Set' in the chapter 'Advanced Configuration'

UI Upload

By Uploading the required .zip files for SchemaSet(s) directly in the UI. For this purpose the SchemaSet subfolders and files (as mentioned in the section 'Adding a new Schema Set') are to be zipped together to a .zip folder. Uploading SchemaSets can be done through the respective configuration page under Configuration → Schemata → Schema Set Upload. By browsing to the .zip folder and uploading this folder the messenger automatically shows the newly uploaded Schema Sets in the messenger UI.



This method involving the UI can be used to 'upgrade' an already existing SchemaSet or to 'import' an new SchemaSet without having to restart the messenger.

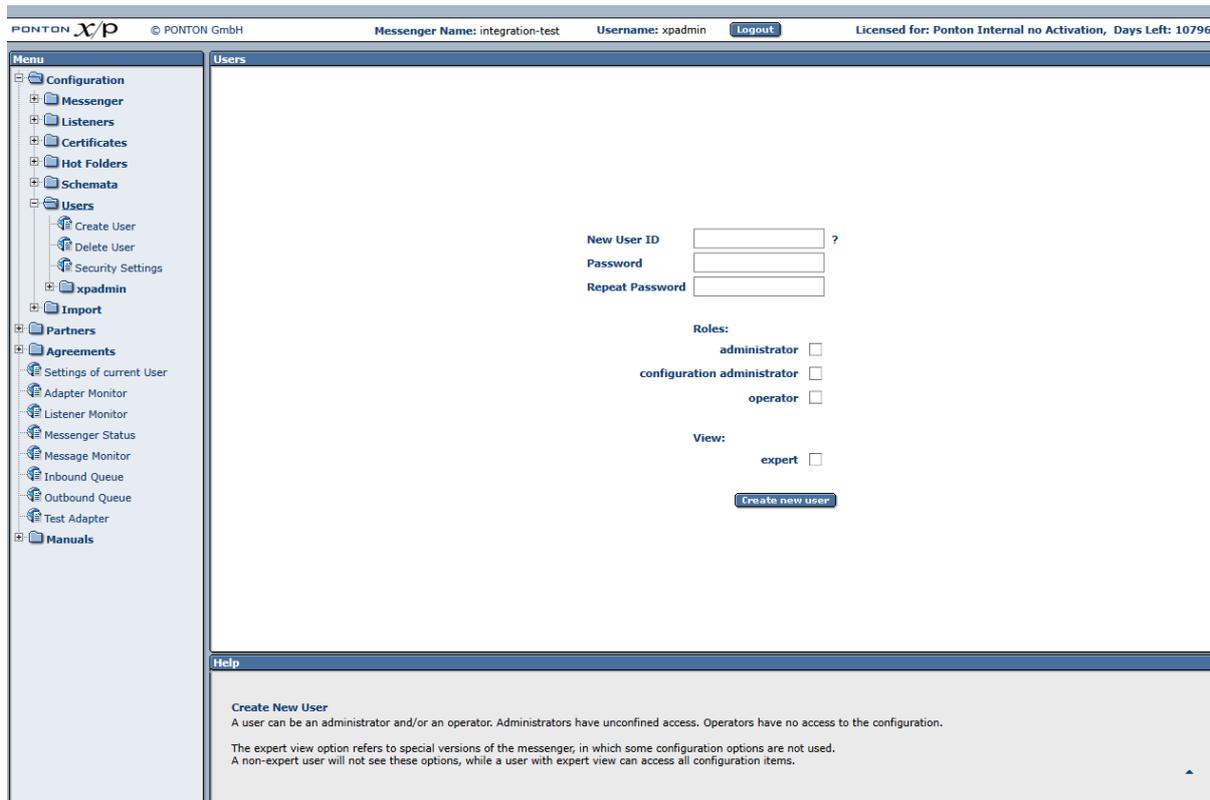
6.6. User Administration

To create, delete or modify existing users for your PONTON X/P installation please navigate to Configuration → Users in the messenger menu.

While creating or editing an existing user there are following types of user roles available to choose from:

- Administrators – these users have full access to the Messenger's configuration interface.
- Configuration Administrators – these users have access to the messenger's configuration interface except for the user configuration section.

- Operators – these users only have access to the Adapter Monitor, the Message Monitor, and the Test Adapter. The options in the configuration menu are not available.



The screenshot shows the X/P Messenger web interface. The top navigation bar includes the PONTON logo, copyright information (© PONTON GmbH), Messenger Name (integration-test), Username (xpadmin), a Logout button, and license information (Licensed for: Ponton Internal no Activation, Days Left: 10796). The left sidebar contains a 'Menu' with various options like Configuration, Messenger, Listeners, Certificates, Hot Folders, Schemata, Users, xpadmin, Import, Partners, Agreements, and Manuals. The main content area is titled 'Users' and displays a 'Create New User' form. The form includes input fields for 'New User ID', 'Password', and 'Repeat Password'. Below these are checkboxes for 'Roles' (administrator, configuration administrator, operator) and 'View' (expert). A 'Create new user' button is at the bottom of the form. A 'Help' section at the bottom of the page provides additional information about user roles and the expert view option.

Create New User
 A user can be an administrator and/or an operator. Administrators have unconfined access. Operators have no access to the configuration.
 The expert view option refers to special versions of the messenger, in which some configuration options are not used. A non-expert user will not see these options, while a user with expert view can access all configuration items.

Additionally, there is a distinction between expert and non-expert users. For the application of the Messenger in some environments certain configuration settings may be pre-defined. In the correspondent Messenger versions these settings are not visible for non-expert users. Nevertheless, expert users can access all items that they are allowed to by their role.

6.6.1. Password Policy

The messenger only allows passwords which comply to the following rules:

Password consists of 12 characters or more, of which there is at least ...

- one UPPER case character
- one lower case character
- one digit
- one special character (!"#\$%&'()*+,-./:;<=>?@[^_`{|})

The new password must be different than the last three passwords.

6.6.2. Password expiry

It is possible to define the expiry period for user passwords. As per default this value is defined as 365 days. To change this value please navigate to Configuration → Users → Security Settings

6.6.3. Account locking

A user account is temporarily locked when the number of failed login attempts exceeds a defined number. The default value of 3 can be adjusted at Configuration → Users → Security Settings

The duration of the temporary lock can also be adjusted on the same page. By default accounts are locked for 1 minutes, to prevent brute force attacks.

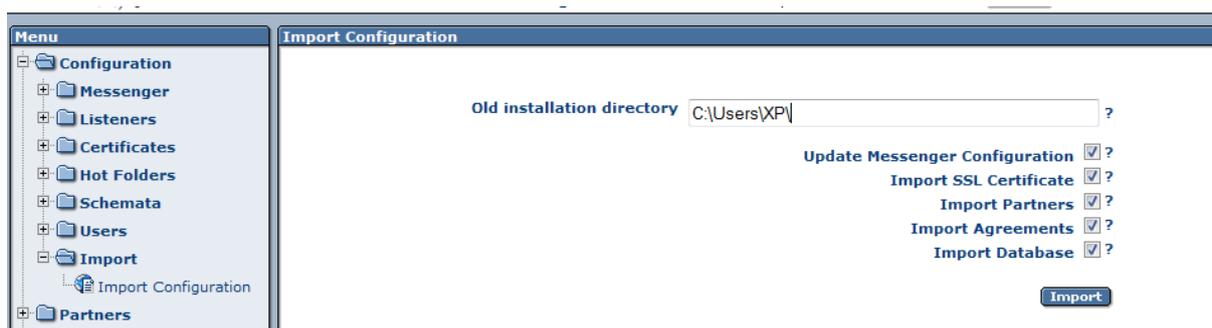
It is possible to set a very large number so that the account lock is effectively permanent.

In both cases it is possible to unlock an account by using an administrator account to reset the password of a locked account.

When an administrator select a user account in the Configuration → Users section, the account lock is visible on the password page.

6.7. Import Configuration

This import enables the migration of older messenger configurations (versions 2.X and lower) into a higher messenger version. To import the configuration please choose Configuration → Import → Import Configuration in the messenger UI.



Following data can be imported:

- Configuration data such as communication settings, partner registry settings, email settings, time servers settings, archive settings etc.
- Partner profiles along with certificates
- Agreements with Partners

- SSL certificates
- Database contents such as message logs from the database schema of the older messenger version. For a detailed description regarding the database import please refer to section 'Database Migration' in the chapter 'Advanced Configuration'.

The message archive itself cannot be automatically transferred. Although you can choose to either leave it where it is and reconfigure the new Messenger to the existing location of this message archive. In that case the old Messenger shall not be in service anymore. Otherwise copy or move the message archive to a different location and configure its new location in the new Messenger.

The target system must have file system access to the source system. If this is not possible due to policy reasons, please create a temporary copy of the old installation on the target file system before starting the configuration import.

6.8. Partner Configuration

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.

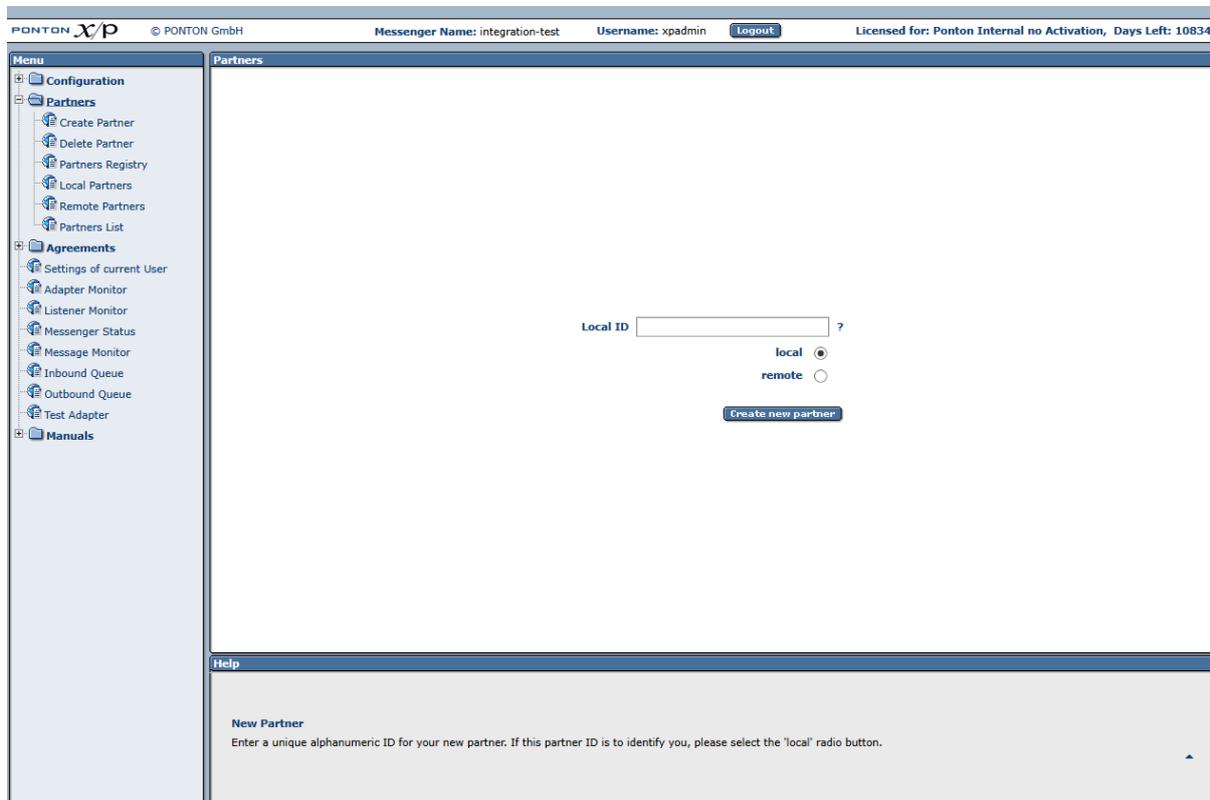
In the case of remote partners you would receive the certificate from the partner directly or by downloading the partner's profile from the registry.

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 (as explained further down) 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.

6.8.1. Create a Partner Entry

To create a new partner entry, go to Configuration → Partners → Create Partner, enter a Local ID for the new partner (this is the local identifier for your configuration) and indicate whether this partner entry is for

- A **local** partner – this might be a department within your organization.
- A **remote** partner – these entries refer to your business partners, for example: customers, suppliers, carriers, warehouse operators, etc.



PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10834

Menu
 Configuration
 Partners
 Create Partner
 Delete Partner
 Partners Registry
 Local Partners
 Remote Partners
 Partners List
 Agreements
 Settings of current User
 Adapter Monitor
 Listener Monitor
 Messenger Status
 Message Monitor
 Inbound Queue
 Outbound Queue
 Test Adapter
 Manuals

Partners
 Local ID ?
 local
 remote
 Create new partner

Help
New Partner
 Enter a unique alphanumeric ID for your new partner. If this partner ID is to identify you, please select the 'local' radio button.

Finally, click on **Create New Partner** to generate the new partner entry – you will then see the partner configuration screen.

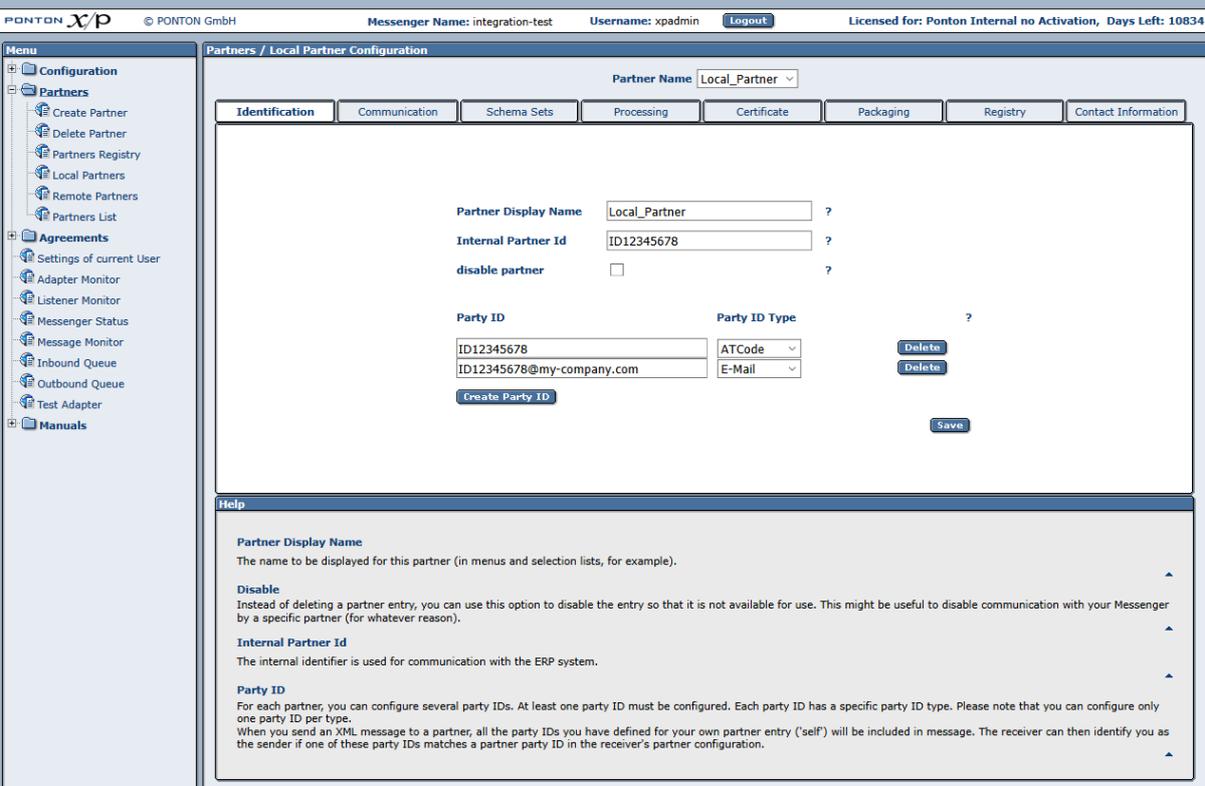
Partner Identification

- **Partner display name** – this is the name shown in the lists and screens within PONTON X/P.
- **Internal 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!
- **Disable** – 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.
- **PartyID / PartyID Type** – PartyIDs 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.

- PartyID Type **Email** is used as the sender's Email address when sending AS1 messages

Note: Please ensure that identical PartyIDs 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. These are configured separately – please check the *Advanced Configuration* section.



Partners / Local Partner Configuration

Partner Name: Local_Partner

Identification | Communication | Schema Sets | Processing | Certificate | Packaging | Registry | Contact Information

Partner Display Name: Local_Partner ?

Internal Partner Id: ID12345678 ?

disable partner: ?

Party ID: ID12345678 | Party ID Type: ATCode ?

Party ID: ID12345678@my-company.com | Party ID Type: E-Mail ?

Buttons: Create Party ID, Delete, Delete, Save

Help

Partner Display Name
The name to be displayed for this partner (in menus and selection lists, for example).

Disable
Instead of deleting a partner entry, you can use this option to disable the entry so that it is not available for use. This might be useful to disable communication with your Messenger by a specific partner (for whatever reason).

Internal Partner Id
The internal identifier is used for communication with the ERP system.

Party ID
For each partner, you can configure several party IDs. At least one party ID must be configured. Each party ID has a specific party ID type. Please note that you can configure only one party ID per type.
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 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.

Identification of Remote Partners

There are a few additional checkboxes on this screen for the configuration of remote partners. 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.

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.

Enabling **automatic Certificate updates** will allow having partner certificates automatically updated if an ebXML signed message is received. Several restrictions apply to this automatic

update:

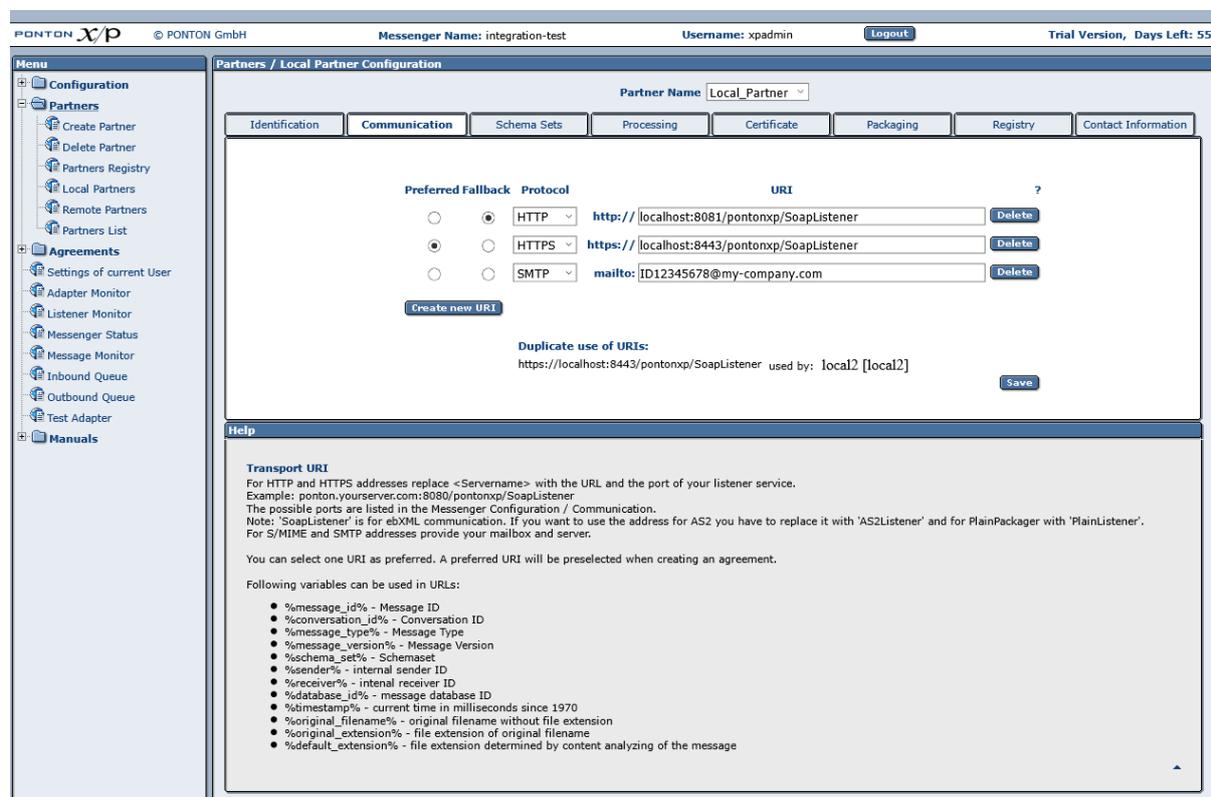
- the new certificate must have a later issue date
 - the issuing CA must be the same
 - the distinguished name of the subject must be unchanged
- Certificate updates via the profile registry are not affected by this flag.

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:
 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
 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.



PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Trial Version, Days Left: 55

Menu

- Configuration
- Partners
 - Create Partner
 - Delete Partner
 - Partners Registry
 - Local Partners
 - Remote Partners
 - Partners List
- Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
- Manuels

Partners / Local Partner Configuration

Partner Name: Local_Partner

Identification Communication Schema Sets Processing Certificate Packaging Registry Contact Information

Preferred Fallback	Protocol	URI	
<input checked="" type="radio"/>	HTTP	http://localhost:8081/pontonxp/SoapListener	Delete
<input type="radio"/>	HTTPS	https://localhost:8443/pontonxp/SoapListener	Delete
<input type="radio"/>	SMTP	mailto:ID12345678@my-company.com	Delete

Create new URI

Duplicate use of URIs:
 https://localhost:8443/pontonxp/SoapListener used by: local2 [local2] Save

Help

Transport URI
 For HTTP and HTTPS addresses replace <Servername> with the URL and the port of your listener service.
 Example: ponton.yourserver.com:8080/pontonxp/SoapListener
 The possible ports are listed in the Messenger Configuration / Communication.
 Note: 'SoapListener' is for ebXML communication. If you want to use the address for AS2 you have to replace it with 'AS2Listener' and for PlainPackager with 'PlainListener'.
 For S/MIME and SMTP addresses provide your mailbox and server.

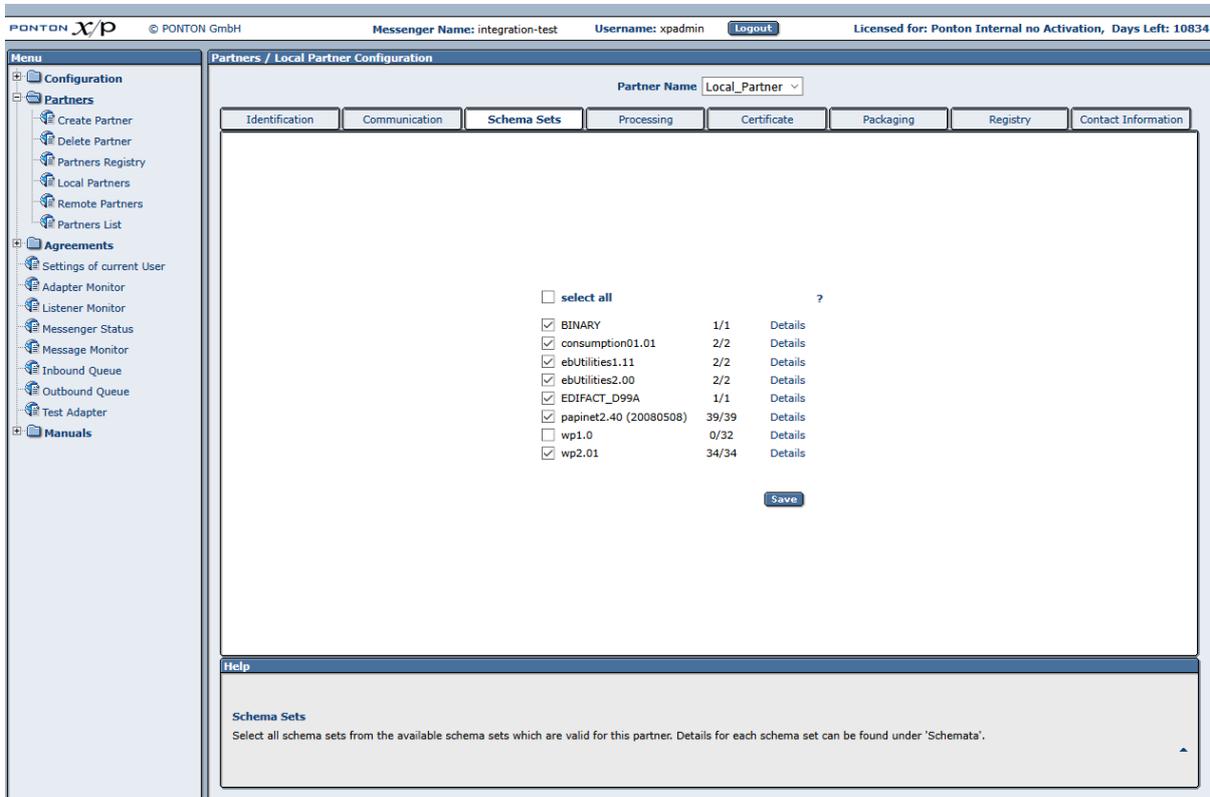
You can select one URI as preferred. A preferred URI will be preselected when creating an agreement.

Following variables can be used in URLs:

- %message_id% - Message ID
- %conversation_id% - Conversation ID
- %message_type% - Message Type
- %message_version% - Message Version
- %schema_set% - Schemaset
- %sender% - internal sender ID
- %receiver% - internal receiver ID
- %database_id% - message database ID
- %timestamp% - current time in milliseconds since 1970
- %original_filename% - original filename without file extension
- %original_extension% - file extension of original filename
- %default_extension% - file extension determined by content analyzing of the message

Schema Sets

The Schema Sets tab allows you to specify which schema sets are "allowed" for message exchange with this partner. The actual set of schemas to be used can be specified individually in each partner agreement.



The screenshot shows the 'Partners / Local Partner Configuration' window. The 'Schema Sets' tab is selected. The partner name is 'Local_Partner'. The interface displays a list of schema sets with checkboxes for selection, a numerical indicator of document types, and a 'Details' link for each entry. A 'select all' checkbox is at the top left of the list. A 'Save' button is at the bottom right of the list area.

Schema Set Name	Document Types	Details
<input type="checkbox"/> select all	?	
<input checked="" type="checkbox"/> BINARY	1/1	Details
<input checked="" type="checkbox"/> consumption01.01	2/2	Details
<input checked="" type="checkbox"/> ebUtilities1.11	2/2	Details
<input checked="" type="checkbox"/> ebUtilities2.00	2/2	Details
<input checked="" type="checkbox"/> EDIFACT_D99A	1/1	Details
<input checked="" type="checkbox"/> papinet2.40 (20080508)	39/39	Details
<input type="checkbox"/> wp1.0	0/32	Details
<input checked="" type="checkbox"/> wp2.01	34/34	Details

Help

Schema Sets
 Select all schema sets from the available schema sets which are valid for this partner. Details for each schema set can be found under 'Schemata'.

On the Schema Sets tab 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.
- 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.
- A Details link that can be used to call up the document type configuration for the given schema set.

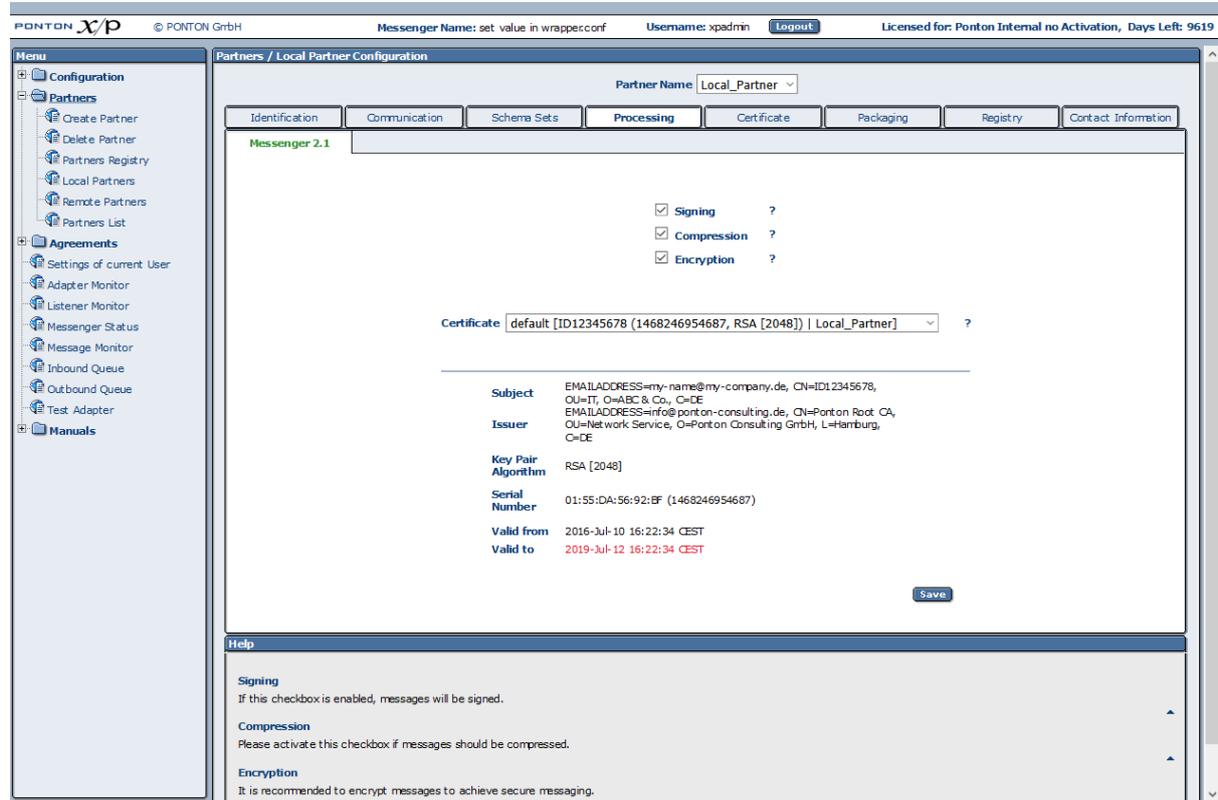
To specify which of the document types contained in a schema set are to be used, click on the Details link. This calls up a window showing a list of the defined document types in the schema set. You can use the checkboxes to activate/deactivate the individual document types. The checkbox above the list (in the upper left corner) can be used as a select all/select none shortcut.

papinet.2.40 (20080508)				
<input checked="" type="checkbox"/>	Type	Version	Location	Namespace
<input checked="" type="checkbox"/>	Availability	V2R40	http://www.papinet.org/v2r40/AvailabilityV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	BookSpecification	V2R40	http://www.papinet.org/v2r40/BookSpecificationV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	BusinessAcceptance	V2R40	http://www.papinet.org/v2r40/BusinessAcceptanceV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	BusinessAcknowledgement	V2R40	http://www.papinet.org/v2r40/BusinessAcknowledgementV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	CallOff	V2R40	http://www.papinet.org/v2r40/CallOffV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	CallOffWood	V2R40	http://www.papinet.org/v2r40/CallOffWoodV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	Complaint	V2R40	http://www.papinet.org/v2r40/ComplaintV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ComplaintResponse	V2R40	http://www.papinet.org/v2r40/ComplaintResponseV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	CreditDebitNote	V2R40	http://www.papinet.org/v2r40/CreditDebitNoteV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	DeliveryInstruction	V2R40	http://www.papinet.org/v2r40/DeliveryInstructionV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	DeliveryMessage	V2R40	http://www.papinet.org/v2r40/DeliveryMessageV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	DeliveryMessageBook	V2R40	http://www.papinet.org/v2r40/DeliveryMessageBookV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	DeliveryMessageWood	V2R40	http://www.papinet.org/v2r40/DeliveryMessageWoodV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	GoodsReceipt	V2R40	http://www.papinet.org/v2r40/GoodsReceiptV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	InfoRequest	V2R40	http://www.papinet.org/v2r40/InfoRequestV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	InventoryChange	V2R40	http://www.papinet.org/v2r40/InventoryChangeV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	InventoryDispositionInstructions	V2R40	http://www.papinet.org/v2r40/InventoryDispositionInstructionsV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	InventoryStatus	V2R40	http://www.papinet.org/v2r40/InventoryStatusV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	Invoice	V2R40	http://www.papinet.org/v2r40/InvoiceV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	InvoiceWood	V2R40	http://www.papinet.org/v2r40/InvoiceWoodV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	LoadAvailable	V2R40	http://www.papinet.org/v2r40/LoadAvailableV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	LoadTender	V2R40	http://www.papinet.org/v2r40/LoadTenderV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	LoadTenderResponse	V2R40	http://www.papinet.org/v2r40/LoadTenderResponseV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	OrderConfirmation	V2R40	http://www.papinet.org/v2r40/OrderConfirmationV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	OrderConfirmationWood	V2R40	http://www.papinet.org/v2r40/OrderConfirmationWoodV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	OrderStatus	V2R40	http://www.papinet.org/v2r40/OrderStatusV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	PackingList	V2R40	http://www.papinet.org/v2r40/PackingListV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	Planning	V2R40	http://www.papinet.org/v2r40/PlanningV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ProductAttributes	V2R40	http://www.papinet.org/v2r40/ProductAttributesV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ProductPerformance	V2R40	http://www.papinet.org/v2r40/ProductPerformanceV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ProductQuality	V2R40	http://www.papinet.org/v2r40/ProductQualityV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	PurchaseOrder	V2R40	http://www.papinet.org/v2r40/PurchaseOrderV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	PurchaseOrderWood	V2R40	http://www.papinet.org/v2r40/PurchaseOrderWoodV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	RFQ	V2R40	http://www.papinet.org/v2r40/RFQV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	RFQResponse	V2R40	http://www.papinet.org/v2r40/RFQResponseV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ScaleTicket	V2R40	http://www.papinet.org/v2r40/ScaleTicketV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ShipmentStatus	V2R40	http://www.papinet.org/v2r40/ShipmentStatusV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	ShippingInstructions	V2R40	http://www.papinet.org/v2r40/ShippingInstructionsV2R40.xsd	http://www.papinet.org/v2r40
<input checked="" type="checkbox"/>	Usage	V2R40	http://www.papinet.org/v2r40/UsageV2R40.xsd	http://www.papinet.org/v2r40

Note: Please click the **OK** button after making any changes to the document type configuration, and then be sure to click the **Save** button on the Schema Set tab. Otherwise your changes will not be saved.

Payload Processing Configuration

The **Validation, Signing, Compression, Encryption** options specify whether the relevant message processing methods are supported by the given partner.



Partners / Local Partner Configuration

Partner Name: Local_Partner

Messenger 2.1

Signing ?
 Compression ?
 Encryption ?

Certificate: default [ID12345678 (1468246954687, RSA [2048]) | Local_Partner] ?

Subject EMAILADDRESS=my-name@my-company.de, CN=ID12345678, OU=IT, O=ABC & Co., C=DE
Issuer EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GrbH, L=Hamburg, C=DE
Key Pair Algorithm RSA [2048]
Serial Number 01:55:DA:56:92:BF (1468246954687)
Valid from 2016-Jul-10 16:22:34 CEST
Valid to 2019-Jul-12 16:22:34 CEST

Help

Signing
If this checkbox is enabled, messages will be signed.

Compression
Please activate this checkbox if messages should be compressed.

Encryption
It is recommended to encrypt messages to achieve secure messaging.

Partner Certificates

Requesting Partner certificates

Requesting a partner certificate is only required for local partners. To obtain a new certificate you can go to the Request tab and fill in the certificate request form to obtain a new certificate from the PONTON CA. You will see a page with a text box containing the certificate request. This page includes an e-mail link that can be used to submit the certificate request to the PONTON CA.

Note: Please remember the private key password so that you can install the requested certificate later.

Installing Partner certificates

Installing partner certificates can be done either by pasting the certificate content as text or by uploading a valid certificate file in the UI. PONTON X/P supports X.509 certificates in binary as well as text format.

Local Partner

After requesting for a new certificate, you shall receive the certificate via Mail from the PONTON CA. When you receive the certificate via e-mail, copy and paste it into the text box on the Show/Install tab. Alternatively you can also upload a valid certificate file as described in the section 'Exporting and Importing certificate files' below.

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.

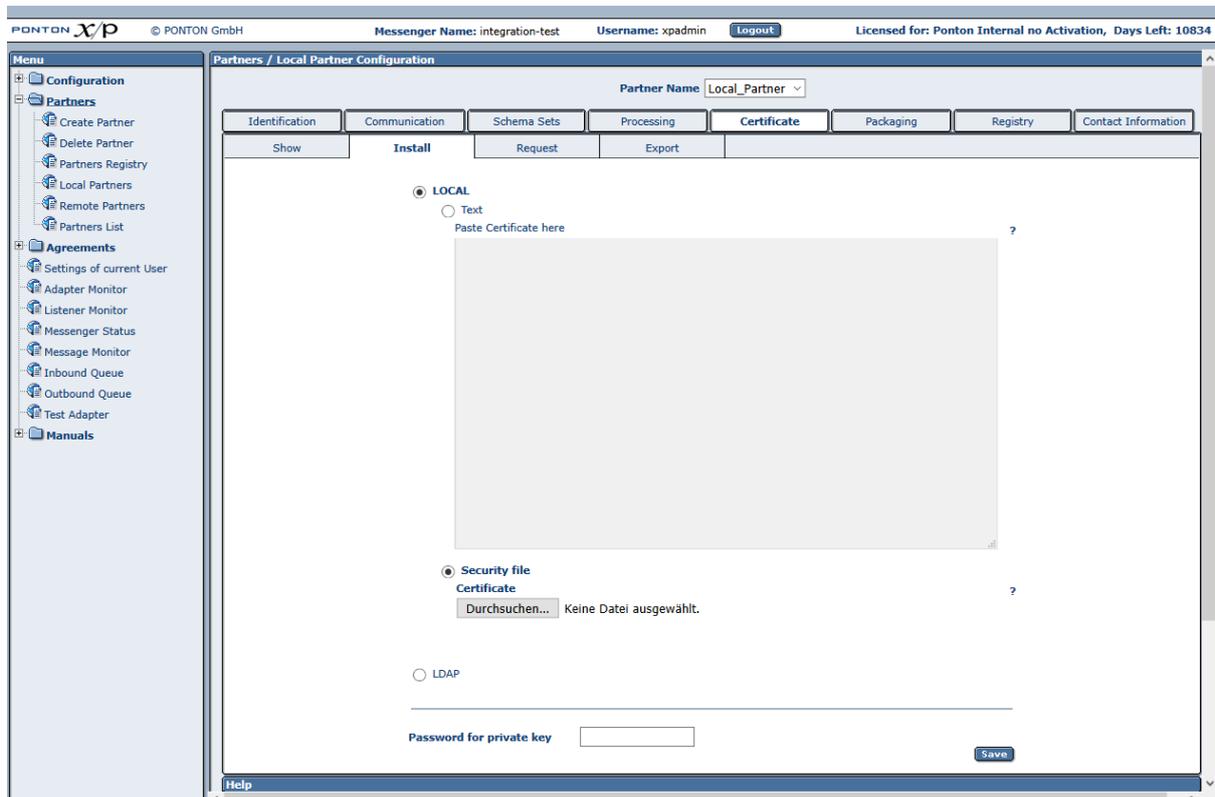
Remote Partner

To install a remote partner's certificate, have the partner send you the certificate via e-mail and then cut and paste the certificate code into the relevant partner configuration. Likewise, you can share your certificate with your business partners by sending the certificate to them via e-mail and having them paste it into their partner configurations. Alternatively you can also upload a valid X.509 certificate file sent to you your communication Partner as described in the section 'Exporting and Importing certificate files' below.

Note: It is important to cut and paste the complete certificate code, *including* the lines "----- Begin Certificate ----" and "----- End Certificate -----".

Important

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.



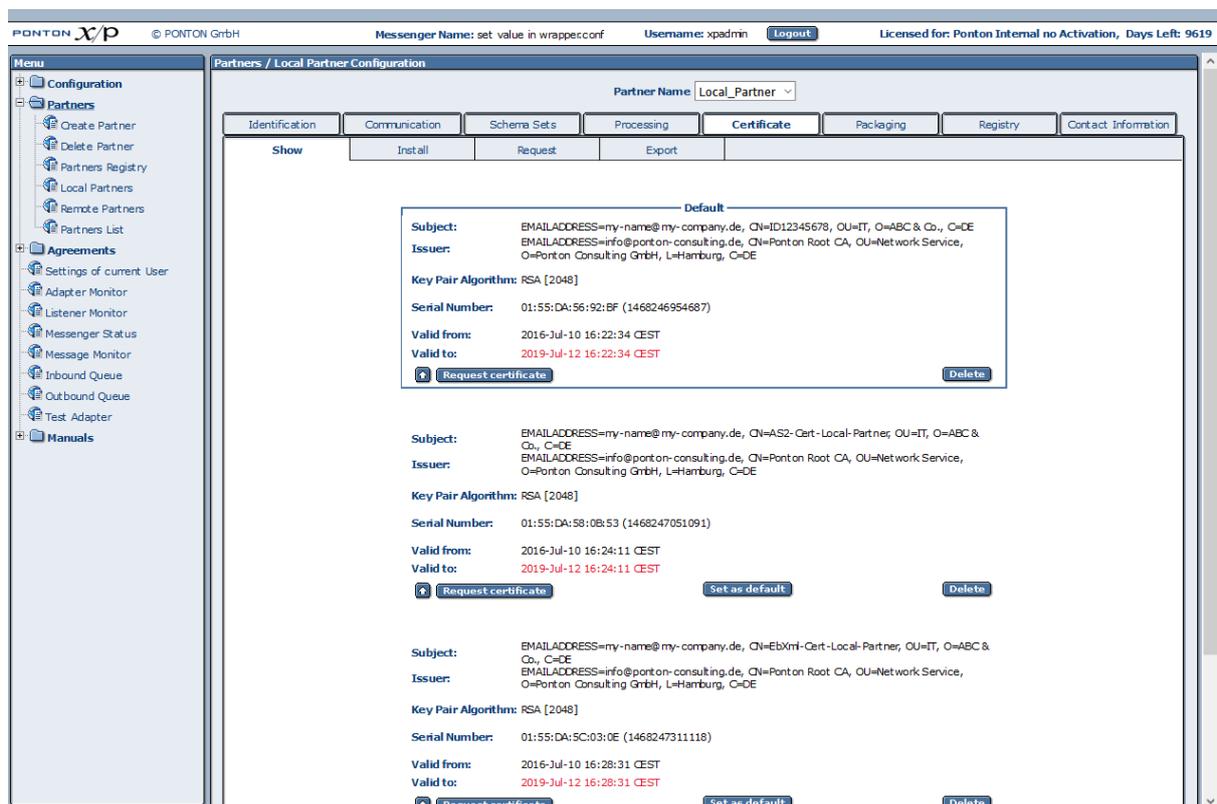
Show installed certificates

You can install **multiple certificates** for partners. This enables you to use different certificates for functions like signing and encryption or for different partners.

Note

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.

For the use of the default certificate function in the agreements, please refer to the 'Partner Agreements' section.



The screenshot shows the 'Partners / Local Partner Configuration' page in the PONTON X/P web interface. The 'Certificate' tab is selected, and the 'Local_Partner' profile is chosen. The interface displays a list of installed certificates with the following details:

Subject	Issuer	Key Pair Algorithm	Serial Number	Valid from	Valid to	Actions
EMAILADDRESS=my-name@my-company.de, CN=ID12345678, OU=IT, O=ABC & Co., C=DE	EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GmbH, L=Hamburg, C=DE	RSA [2048]	01:55:DA:56:92:BF (1468246954687)	2016-Jul-10 16:22:34 CEST	2019-Jul-12 16:22:34 CEST	Request certificate, Delete
EMAILADDRESS=my-name@my-company.de, CN=AS2-Cert-Local-Partner, OU=IT, O=ABC & Co., C=DE	EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GmbH, L=Hamburg, C=DE	RSA [2048]	01:55:DA:58:0B:53 (1468247051091)	2016-Jul-10 16:24:11 CEST	2019-Jul-12 16:24:11 CEST	Request certificate, Set as default, Delete
EMAILADDRESS=my-name@my-company.de, CN=EbXml-Cert-Local-Partner, OU=IT, O=ABC & Co., C=DE	EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GmbH, L=Hamburg, C=DE	RSA [2048]	01:55:DA:5C:03:0E (1468247311118)	2016-Jul-10 16:28:31 CEST	2019-Jul-12 16:28:31 CEST	Request certificate, Set as default, Delete

Exporting / Importing certificate files

Exporting an installed certificate

Exporting a certificate as follows enables you to save and then reuse your own certificate as long as it is valid. Please navigate to the menu Partner → Local Partner and choose the required local Partner profile <local_Partner> from the drop down list. In the Tab Certificate → Export choose the required certificate from the drop down list next to 'Certificate Alias' and feed the Private Key Password for this particular certificate. 'Download' and Save the file. This leads to a .p12 file, which is the required private certificate. This certificate file can also be used for other local partners in the same or different messenger but only along with the Private Key Password.

Alternatively, if you wish to export and exchange your partner certificate with remote communication partners simply 'Download' the required certificate without feeding the Private Key Password. This will lead to a .der file, which is the required public certificate.

Importing and installing a certificate file

To import a certificate file for a local partner in the messenger, please navigate to the messenger menu Partner → Local Partner and choose the required local Partner profile <local_Partner>. In the Tab Certificate → Install choose the option 'Security File Certificate' and 'Browse...' the required certificate file. Feed the Private Key Password for this particular certificate and click 'Save'.

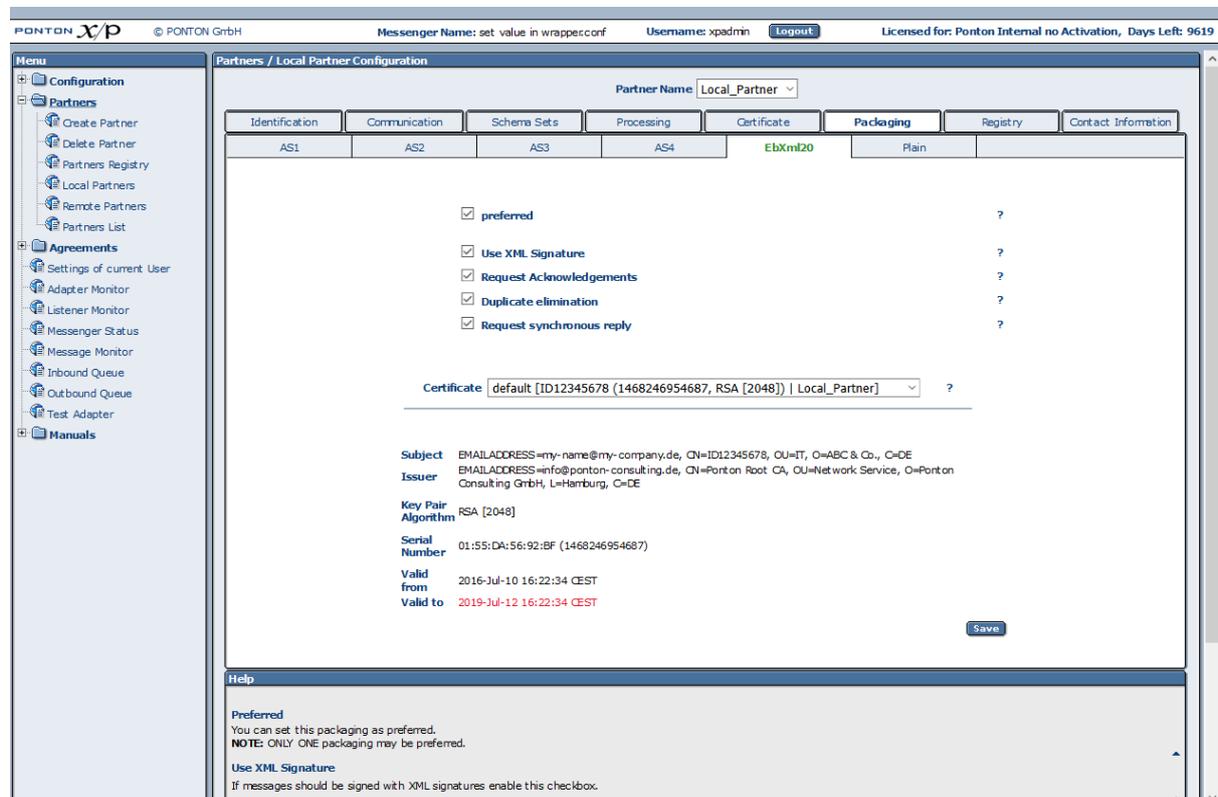
Alternatively, if you wish to import and install a certificate file for a remote partner simply Browse...' the required certificate file and click 'Save'.

Message Packaging

The options on this page specify how the messages sent by this 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 profile.

Note: 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.

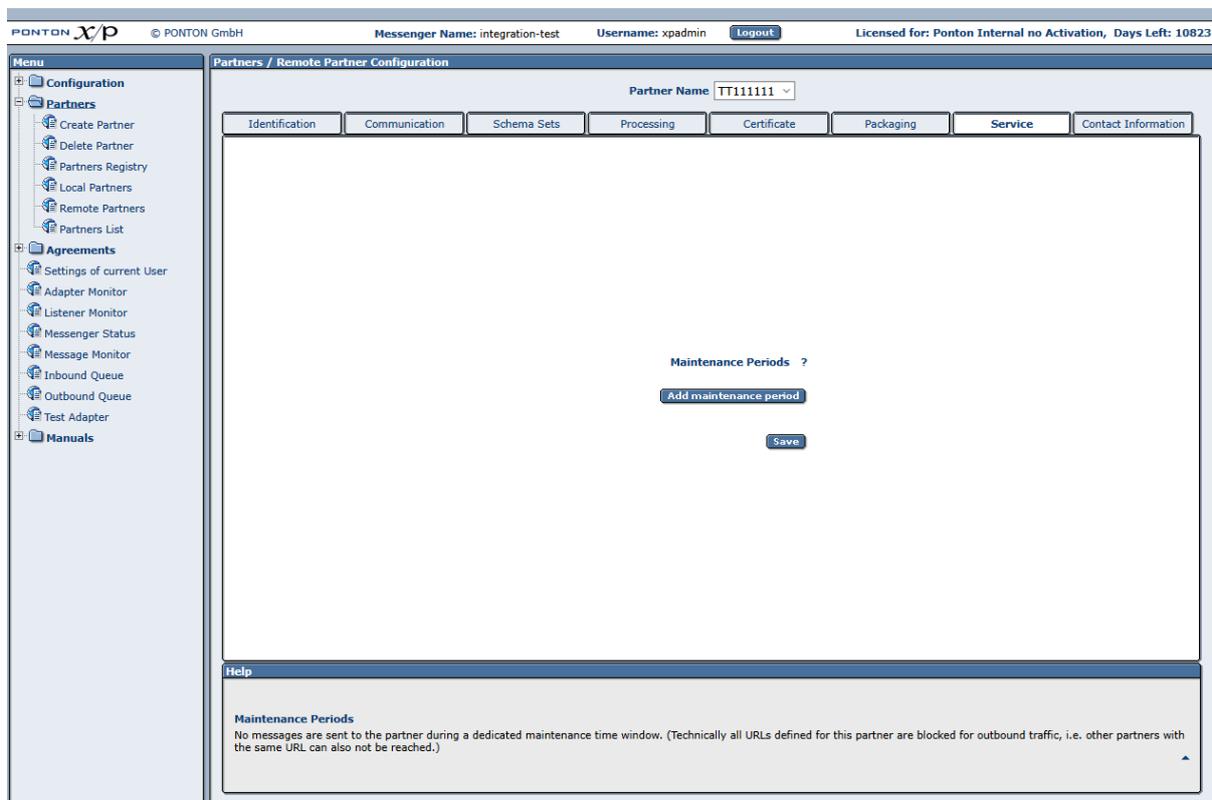


The screenshot displays the 'Partners / Local Partner Configuration' page for 'Local_Partner'. The interface includes a navigation menu on the left and a main configuration area with tabs for Identification, Communication, Schema Sets, Processing, Certificate, Packaging, Registry, and Contact Information. The 'Packaging' tab is selected, showing a table with columns for AS1, AS2, AS3, AS4, EbXml20, and Plan. Below the table, there are several checked options: 'preferred', 'Use XML Signature', 'Request Acknowledgements', 'Duplicate elimination', and 'Request synchronous reply'. A 'Certificate' dropdown menu is set to 'default [ID12345678 (1468246954687), RSA [2048]] | Local_Partner'. Below this, there is a 'Subject' field with the value 'EMAILADDRESS=my-name@my-company.de, CN=ID12345678, OU=IT, O=ABC & Co., C=DE' and an 'Issuer' field with the value 'EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GmbH, L=Hamburg, C=DE'. The 'Key Pair Algorithm' is set to 'RSA [2048]', the 'Serial Number' is '01:55:DA:56:92:BF (1468246954687)', the 'Valid from' date is '2016-Jul-10 16:22:34 CEST', and the 'Valid to' date is '2019-Jul-12 16:22:34 CEST'. A 'Save' button is located at the bottom right of the configuration area. A 'Help' section at the bottom provides additional information about the 'Preferred' and 'Use XML Signature' options.

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.

Remote Maintenance

Remote Maintenance is used for disable message exchange with the remote partner. To enable remote maintenance, at least one maintenance period must be created. During this time the Messenger will not send any documents/pings to the partner.



The screenshot shows the PONTON X/P Messenger interface. The top bar displays 'Messenger Name: integration-test', 'Username: xpadmin', and 'Licensed for: Ponton Internal no Activation, Days Left: 10823'. The left sidebar contains a 'Menu' with categories like Configuration, Partners, Agreements, and Manuals. The main area is titled 'Partners / Remote Partner Configuration' and shows a dropdown for 'Partner Name' set to 'TT1111111'. Below this are several tabs: Identification, Communication, Schema Sets, Processing, Certificate, Packaging, Service, and Contact Information. The 'Service' tab is selected, displaying a 'Maintenance Periods' section with a question mark icon, an 'Add maintenance period' button, and a 'Save' button. A 'Help' section at the bottom provides details: 'Maintenance Periods: No messages are sent to the partner during a dedicated maintenance time window. (Technically all URLs defined for this partner are blocked for outbound traffic, i.e. other partners with the same URL can also not be reached.)'

Synchronize Partner Profile with the Registry

To synchronize the current partner configuration with the profile 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. Otherwise you will see an **Upload**-button (in case of a local partner) or a **Download**-button (in case of a remote partner).

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. For this reason you may experience a short delay when you open the Registry tab.

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10823

Menu

- Configuration
 - Partners
 - Create Partner
 - Delete Partner
 - Partners Registry
 - Local Partners
 - Remote Partners
 - Partners List
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manually

Partners / Local Partner Configuration

Partner Name: Local_Partner

Identification | Communication | Schema Sets | Processing | Certificate | Packaging | **Registry** | Contact Information

Upload partner profile to registry ?

Local partner profile is newer than the partner profile on the registry server. The partner profile on the registry server should be updated.

Local profile	Profile in registry
Last modified 2016-07-11 16:28:59 CEST	Last modified No profile available

Help

Upload partner profile to registry

If the local partner profile was modified, it is possible to upload it to the registry server.

6.8.2. Delete a Partner Entry

To delete a partner entry, go to Configuration → Partners → Delete Partner, select the relevant Partner Name (the display name in your configuration), and then click **Delete Partner**.

6.8.3. Using the Partner Registry

If your communication partners and you have a common partners registry then exchanging partner profiles can be very simple.

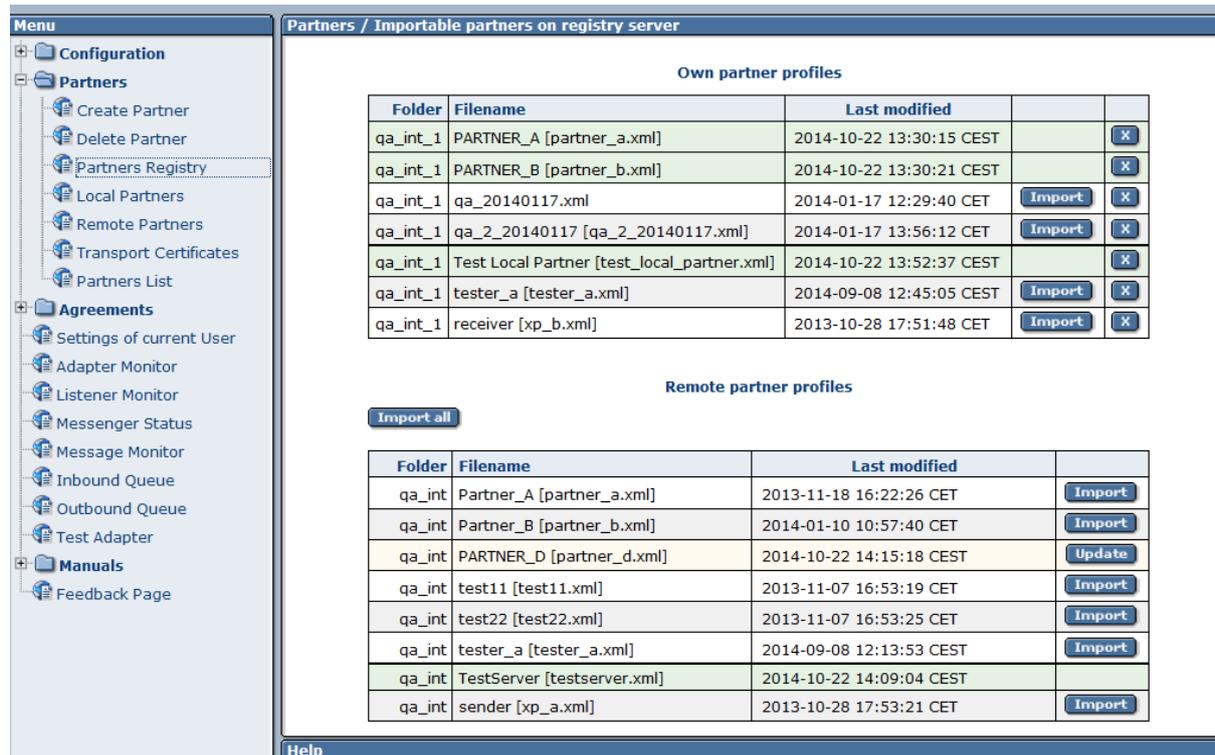
Download all profiles

To download all available profiles navigate to Partners → Partners Registry and click 'Import all'. This automatically imports all available profiles from the registry into your local messenger. Although, profiles which may collide within already existing profiles within your messenger will not be imported to avoid overwriting current profiles.

Update individual profiles

Profiles which have been modified since the last import are highlighted under Partners → Partners Registry and have a button 'update' next to them. By clicking 'update' these modified profiles are automatically downloaded into the messenger.

Alternatively, you could activate the option 'Automatic updates' to enable your messenger to update all downloaded profiles periodically as described in the section 'Partner Registry Configuration'



Partners / Importable partners on registry server

Own partner profiles

Folder	Filename	Last modified		
qa_int_1	PARTNER_A [partner_a.xml]	2014-10-22 13:30:15 CEST		X
qa_int_1	PARTNER_B [partner_b.xml]	2014-10-22 13:30:21 CEST		X
qa_int_1	qa_20140117.xml	2014-01-17 12:29:40 CET	Import	X
qa_int_1	qa_2_20140117 [qa_2_20140117.xml]	2014-01-17 13:56:12 CET	Import	X
qa_int_1	Test Local Partner [test_local_partner.xml]	2014-10-22 13:52:37 CEST		X
qa_int_1	tester_a [tester_a.xml]	2014-09-08 12:45:05 CEST	Import	X
qa_int_1	receiver [xp_b.xml]	2013-10-28 17:51:48 CET	Import	X

Remote partner profiles

Import all

Folder	Filename	Last modified		
qa_int	Partner_A [partner_a.xml]	2013-11-18 16:22:26 CET	Import	
qa_int	Partner_B [partner_b.xml]	2014-01-10 10:57:40 CET	Import	
qa_int	PARTNER_D [partner_d.xml]	2014-10-22 14:15:18 CEST	Update	
qa_int	test11 [test11.xml]	2013-11-07 16:53:19 CET	Import	
qa_int	test22 [test22.xml]	2013-11-07 16:53:25 CET	Import	
qa_int	tester_a [tester_a.xml]	2014-09-08 12:13:53 CEST	Import	
qa_int	TestServer [testserver.xml]	2014-10-22 14:09:04 CEST		
qa_int	sender [xp_a.xml]	2013-10-28 17:53:21 CET	Import	

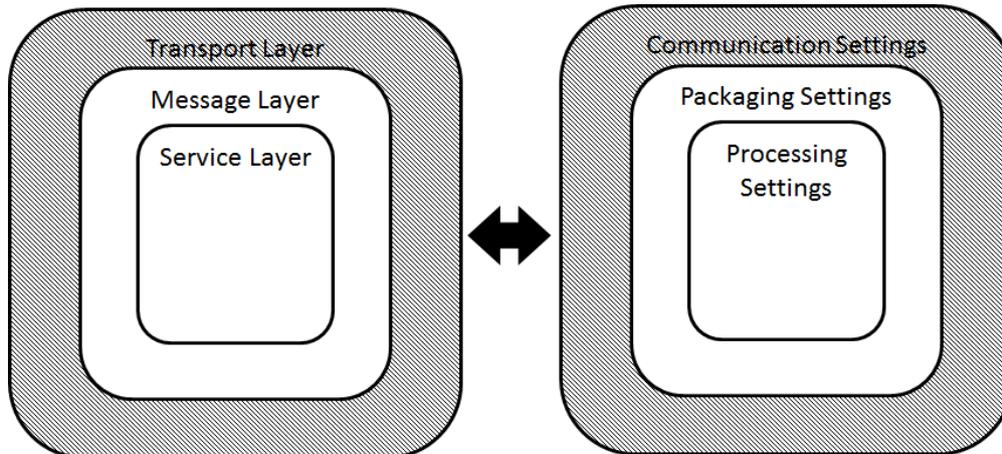
6.9. Partner Agreements

Partner agreements serve 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 local and a remote partner.

When setting up a partner agreement it should be noted that the options available for selection depends on the options supported by the individual profiles of these two partners. Only options that are activated in both partner configurations can be chosen as part of the partner agreement.

The agreements define specific settings relating to the End-to-End exchange of messages between the partners. Within an agreement information regarding the communication, standardised packaging as well as file processing are defined between two partners as

required by the transport layer, message layer as well as the service layers while communicating



6.9.1. Creating a Partner Agreement

To create a new partner agreement, go to Configuration → Agreements → Create/Delete Agreement.

- From the list of Local and Remote Partners, select your local partner and the intended remote partner for this new agreement. Then click on **Create New Agreement**.
- This leads you to the agreement configuration page. You can call up this page afterwards by going to Configuration → Agreements → Agreements and selecting the relevant partners at the top of the page or by clicking on an entry in the Agreements List (Configuration → Agreements → Agreements List).

Creating an Agreement between two local partners

To be able to create an agreement between two local partners you first have to enable loopback in the communication configuration of the Messenger as described in the section 'Communication Settings'.

Only one agreement is created between two local partners. This means that most settings are fixed for inbound direction of the receiving partner after adjusting the sender's outbound settings. Nevertheless, you have to change the roles of partner1 and partner2 when editing the agreement once to define the inbound adapter the receiving partner should use.

6.9.2. Editing a Partner Agreement

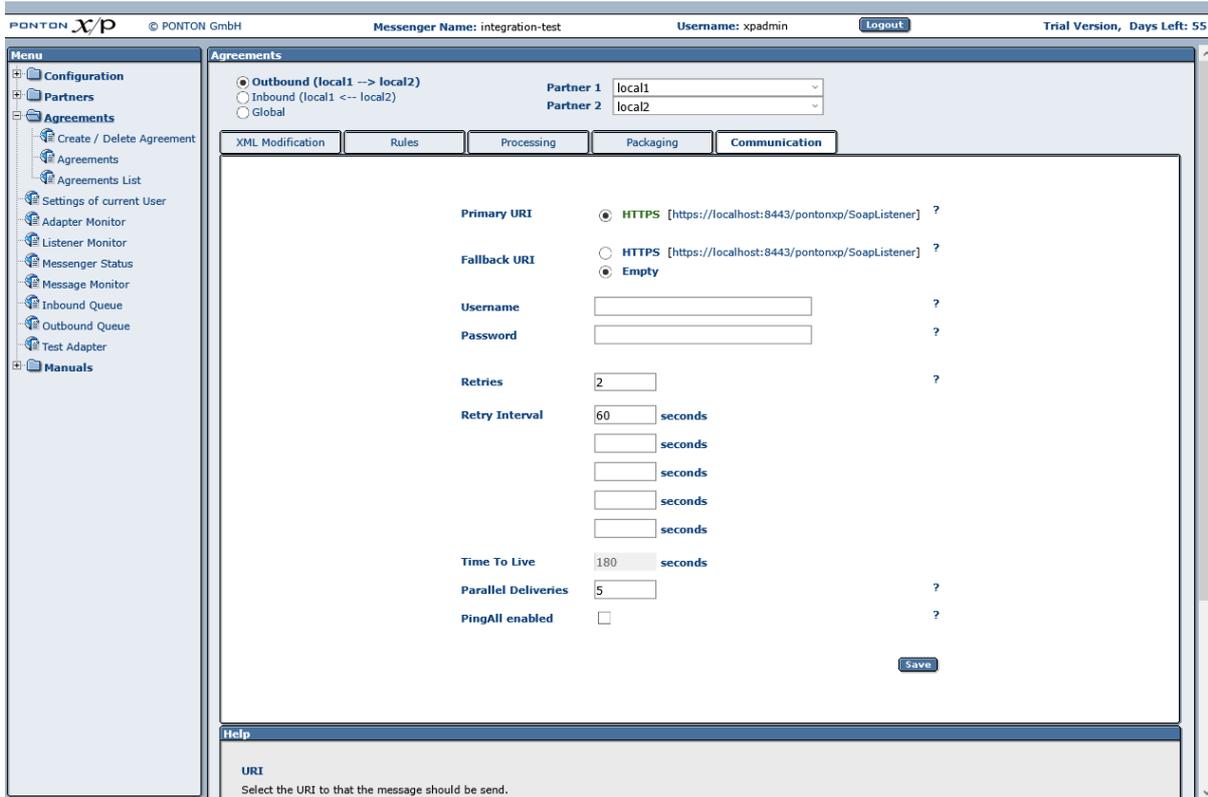
To display or edit the settings in an existing partner agreement, go to Configuration → Agreements → Agreements. From the list of Local and Remote Partners at the top of the screen, select the partners the agreement applies to. Then click the **Outbound**, **Inbound** or **Global** radio button (in the upper left corner) to call up the respective settings for this agreement:

- **Outbound** – these settings apply to (outgoing) messages that partner1 sends to partner2. These settings include further settings for Packaging, Communication etc.
- **Inbound** – these settings apply to (incoming) messages that partner1 receives from partner2. These settings also include further settings for Packaging, Communication etc.
- **Global** – these settings apply to both outbound and inbound messages and define the schema sets (and thereby the documents) to be exchanged between partner1 and partner2.

While preparing the messages for outbound communication the agreement settings are applied sequentially in the following order - XML Modification, Rules, Processing, Packaging and then Communication. In case of incoming messages the agreement settings are applied in the order - Packaging, Processing, XML Modification, Rules and then Communication.

Primary functions of these settings are as follows:

- XML Modification: Optional setting if special treatment is required for xml files received from / delivered to the backend.
- Rules: Optional setting to define special treatment for files with certain contents etc.
- Processing: Optional settings to sign and/or (de-) en-encrypt the file (or payload).
- Packaging: These settings are mandatory to define. Since they define the messaging standard to be applied. Further options within the chosen setting are optional to choose from.
- Communication: These settings are mandatory to define. Since they define the communication path for message delivery.
 - Fallback : In case the partner is reachable at more than one URI, a fallback URI can be defined in the partner agreements. The messenger will use the fallback URI only if the primary URI has been identified as unreachable during the previous transmission tries. The fallback channel is only used if "PingAll" option is enabled in the agreement as well as globally under Configuration → Messenger → Communication.



The screenshot shows the PONTON X/P Messenger configuration interface. The top bar displays 'Messenger Name: integration-test', 'Username: xpadmin', and 'Logout'. The left sidebar contains a 'Menu' with options like Configuration, Partners, Agreements, and Manuals. The main area is titled 'Agreements' and shows settings for an 'Outbound (local1 --> local2)' agreement. The 'Communication' tab is active, showing fields for Primary URI (selected as HTTPS), Fallback URI (selected as Empty), Username, Password, Retries (2), Retry Interval (60 seconds), Time To Live (180 seconds), Parallel Deliveries (5), and PingAll enabled (unchecked). A 'Save' button is at the bottom right. A 'Help' section at the bottom left explains the URI field: 'URI Select the URI to that the message should be send.'

Please note, that an agreement has to be compatible on both sides (partner1 as well as partner2). So you will want to contact the partner2 to specify the options to be supported. Options that are not supported by any of the partners are seen with a red **X** at the top of the agreement configuration Screens. The required settings to rectify these will be highlighted in red text next to the respective options. Please deactivate any settings in the agreement that are not supported by both partners. Section 'Locating Inconsistencies in a Partner Agreement' in the chapter advanced configuration deals with this in more detail.

Profiles imported from the profile registry should not be changed locally since they might be overwritten with the next update. You will have to contact the relevant partner, agree on a common set of configuration options, and then upload & update modified configurations via the profile registry.

Communication

These settings are defined quite differently depending on the direction of communication.

Outbound

In case of outbound communication following options are available:

- **URI** – specifies the transport protocol to be used for sending messages based on this agreement. It is mandatory to choose one URI.

- Username / Password – only needs to be provided if the URI can only be accessed after authentication.
- **Retries / Retry Interval** – indicates how often and how long the Messenger will try to send a message until it receives an acknowledgement. If more than (retries + 1) intervals are entered than the last retry interval will be used by rest retries.
- **PingAll enabled** – enables the user to monitor the reachability of partner2 in pre-defined intervals. By activating this option in agreements a report will be generated which includes the PING results and provides these results to an external monitoring tool. For further description regarding this please refer to the section 'Application Monitoring (JMX)' in the advanced configuration.
- **Parallel deliveries** – defines the number of parallel connections allowed towards partner2 to deliver outgoing messages. It is recommended to define a value between 1 - 5. The value allowed here depends on the availability of ports on the installed server and the configuration of network components such as firewalls etc.

Inbound

In case of inbound communication only an adapter such as 'hotfolder' needs be chosen, which shall deliver the incoming messages to the backend application.

Packaging

Packaging configuration allows you to apply globally defined standards to communicate with external parties. The PONTON X/P Messenger supports ebXML, AS1, AS2, AS3 and AS4. Furthermore the messenger also allows exchange of plain messages.

ebXML

It is a standard available for multiple protocols. Within the messenger following options are available to make messaging more compatible between individual parties, since different parties might only accept / send messages which fulfill certain criteria :

- **XML Signature** – signs the message with XML Signature. In the outbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your local partner.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as EbXml) configuration of the local partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the local partner profile is changed.
- **Request Acknowledgements** – to allow incoming Acknowledgements (ebXML Signal message) to be processed successfully. This acknowledgement from your partner. These acknowledgements can be signed, if your partner supports this option.

- The **ebXML Service / ebXML ServiceType** settings can be used to specify the ebXML service that handles the message. For papiNet messaging "%TESTFLAG%" can be used as the service identifier (to automatically set the service to Test or Production) and "papiNet" can be used as the service type.
- **ebXML Action** – This setting identifies a process within the specified ebXML Service. For papiNet messaging "%MESSAGE TYPE%" can be used to automatically set the action to the message type.
- **Duplicate elimination** – If duplicate elimination is set, the receiving messenger must eliminate duplicate messages. If not set, duplicate messages are not required to be eliminated.
- **Request synchronous reply** – If you use a synchronous protocol, a reply can be requested through the same connection.
- **CPA Id** – The CPA Id specifies the parameters governing the exchange of messages between the parties. For papiNet messaging the following agreement can be used: www.papiNet.org/data/CPABasicHTTP.xml.
- **Role** – EbXml allows you to define a role for sender and receiver (ex. 'buyer' and 'seller'). This has no effect on PONTON X/P, but other messaging software might require specific values.
- **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.

AS1, AS2, AS3

The possible settings for these standards are mostly the same, but while AS1 is available for SMTP, AS2 covers the communication by HTTP(S) and AS3 covers the communication by FTP(S).

- **Request Acknowledgement** – you can request an MDN (Message Disposition Notification) for all outbound messages from your partner. If you want the MDN to be signed, you can select the algorithm.
 -  If the receiver of your Messages via AS1 is not able to / willing to send standard compliant MDNs you can also activate the Option 'SMTP Response' in the agreement. By activating this option your own Messenger will automatically create an ACK message for your backend application as soon as the outbound message has been successfully delivered to your SMTP server.
- For AS2, the MDN can be send to an address different to the sender address, if you enable **Request asynchronous reply** and fill in the URI.
- **S/MIME signature** – you can select the algorithm to sign the message with your **partner certificate**. In the outbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your local partner.

- the selected algorithm uses "PKCS1-v1_5" unless "PSS" is specifically mentioned
- Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as AS2) configuration of the local partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the local partner profile is changed.
-  For **AS2 S/MIME MDN Signature** algorithm can be defined separately as per algorithm requirements of the remote partner for MDNs.
- If you enable **S/MIME compression** less data has to be transmitted at the cost of more CPU load.
- **S/MIME encryption** – It is recommended to encrypt messages to achieve secure messaging. Your message will be encrypted with your partner's **certificate**.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as AS2) configuration of the remote partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the remote partner profile is changed.
 - The default encryption algorithm is "DES_EDE_CBC", this can be changed by enabling the **Algorithm option** and selecting a different algorithm like AES256_CBC.
 - When using OAEP encryption, there is a hash algorithm used during encryption. The used hash algorithm is denoted behind the OAEP tag. (ex. "OAEP_SHA256")

Extended AS1 Options

- **Subject** – This option defines the subject for all outgoing mails.
- **With Body** – The messenger creates a body part with a defined text for all outgoing mails.
- **Mail Client Support** – 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).

AS4

Following settings are possible and can be defined while using the AS4 standard in the messenger :

- **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.
- **AgreementRef** – The value of an AgreementRef element identifies the agreement that governs the exchange and must be unique within a namespace mutually agreed by the two parties.
 - **AgreementRefType** - This OPTIONAL 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

Furthermore following variables can be used in the options **Role To** , **Role From**, **Service**, **Service Type**, **Action**, **AgreementRef** as well as **AgreementRefType**:

%MESSAGE%TYPE%, %TESTFLAG%, %MESSAGEVERSION%, %SCHEMASET%,
 %SENDERID%, %SENDER_DISPLAYNAME%, %RECEIVERID%,
 %RECEIVER_DISPLAYNAME%, %MESSAGEID%, %CONVERSATIONID%

- **Include 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.
- **Include Content-Properties** – If this is enabled, then payload related information is added to the AS4 envelope as Type/Value pairs.
- **Certificate Update** – If a new certificate is installed in a local 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 Message** – 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.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as EbXml) configuration of the local partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the local partner profile is changed.

- **Encrypt Message** – You can select the algorithm to encrypt the message with your partner's Certificate. In the inbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your remote partner.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as EbXml) configuration of the remote partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the remote partner profile is changed.
 - **Key Info** – This allows the user to choose one out of the three possible modes for communicating Key Infos to your partners
- **Compress Message** – You can select to compress the message before sending.
- **Expect Receipt** – It can be specified to expect a receipt stating successful delivery of messages. The expected receipt could be signed or unsigned. The algorithm required for signing could also be specified here.

Plain

Is available for HTTP(S) and FTP(S). Plain packaging allows sending and receiving pure XML messages without the need of a transport envelope. This packaging option is intended for the communication with a partner that does not have a Messaging software. Setup for plain packager is described in more detail in the section 'Agreement Configuration for Plain Packager' in the chapter advanced configuration.

Processing

All options selected under processing are applied to the payload.

- **Validation** – enables XML validation for incoming/outgoing messages.
- **Signing** – specifies whether signing is to be used. If activated you can select the signature algorithm: "SHA1withRSA", "SHA512withRSA", "MD5withRSA" or "SMIME-SHA1". In the outbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your local partner.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as EbXml) configuration of the local partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the local partner profile is changed.
- **Compression Type** – specifies whether compression is to be used. If activated, you can select the compression type: "Zlib", "Deflated" , "GZIP" and "ZIP". The default value is "Zlib".

- **Encryption** – It is recommended to encrypt messages to achieve secure messaging. Selectable values are DES-EDE3-CBC, SMIME-DES-EDE3-CBC, AES256_CBC or SMIME-AES256_CBC. Encryption is performed with your remote partner's certificate. In the inbound direction you can select one specific certificate for signing in case you have installed multiple certificates for your remote partner.
 - Other than choosing a specific certificate it is also possible to choose a 'default' packager certificate. Default packager certificate refers to the chosen certificate in the specific packager (such as EbXml) configuration of the remote partner profile. It could be helpful to choose 'default' if you wish to automatically update the certificate in the agreement as soon as the certificate in the specific packager configuration of the remote partner profile is changed.

You can select divergent processing options for special Message Types by defining Processing Exceptions.

Rules

The settings on this tab can be used to specify Content Rules for inbound and outbound messages based on the current partner agreement. The Inbound / Outbound radio buttons are used to display the settings for the respective message processing direction. For details please refer to the section *Content Rules* in the Chapter Advanced Configuration.

XML Modification

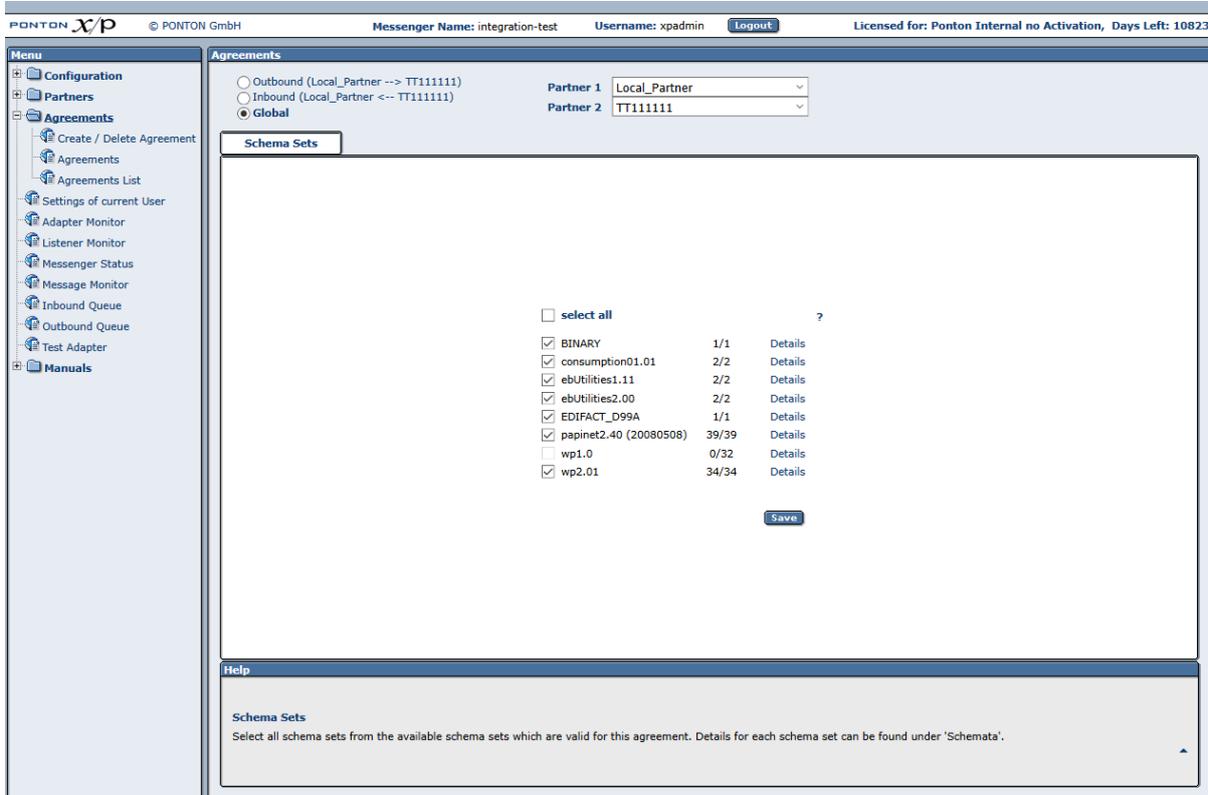
XML Modification enables change in encoding and the line ending of a document before sending or after receiving it, so that it is adapted to the requirements of the receiver or of an interior adapter.

Additionally, there are options to change some XML elements in the payload that are especially helpful to guarantee the compatibility with older papiNet standards.

- **XML Encoding** – the document can be transferred to UTF-8 and UTF-16, several ISO encodings and some encodings for Japanese text.
- **Line Ending** – the line endings in the document will be changed to the LF, CR or CR LF.
- **Update Envelope** – 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.
- **Doctype** – the DTD in a payload document can be updated according to the schema or can be 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.

Schema Sets

The Schema Sets tab 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 tab open the relevant partner agreement and click the **Global** settings button.



The screenshot shows the X/P Messenger interface. The top bar includes the logo, version, and user information. The left menu is expanded to 'Agreements'. The main area shows the 'Agreements' configuration for a partner agreement. The 'Global' radio button is selected. The 'Schema Sets' tab is active, displaying a list of schema sets with checkboxes for selection. A 'Save' button is at the bottom right of the list.

Schema Set	Version	Status	Details
<input type="checkbox"/> select all			
<input checked="" type="checkbox"/> BINARY	1/1		Details
<input checked="" type="checkbox"/> consumption01.01	2/2		Details
<input checked="" type="checkbox"/> ebUtilities1.11	2/2		Details
<input checked="" type="checkbox"/> ebUtilities2.00	2/2		Details
<input checked="" type="checkbox"/> EDIFACT_D99A	1/1		Details
<input checked="" type="checkbox"/> papinet2.40 (20080508)	39/39		Details
<input type="checkbox"/> wp1.0	0/32		Details
<input checked="" type="checkbox"/> wp2.01	34/34		Details

Help

Schema Sets
 Select all schema sets from the available schema sets which are valid for this agreement. Details for each schema set can be found under 'Schemata'.

Please note that the schema sets available for selection in a given partner agreement are dependent on the basic settings in your partner profiles for the two relevant partners. In the above example, the schema set for *X12_503* cannot be activated, because one of the partner profiles does not support this schema set. 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 remote partners you will need to cross check the selected options (as well as your other configuration settings) with your partners.

For further details, please refer to Partner Configuration → Schema Sets.

7. Advanced Configuration

This Section deals primarily with issues relevant for the advanced configuration and troubleshooting the Messenger if required.

7.1. Listener Configuration

To securely transmit messages between the Messenger and the internet 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 between the Listener and the Messenger.

i Please note that if you are going to receive incoming connections via the Listener, your partners will have to enter the public URI of your Listener in their configurations (under Configuration → Partners → <partner name> → Communication Tab → URI of Partner's Messenger Service).

7.1.1. 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. The configuration is carried out in the Messenger Admin tool.

7.1.2. Listener Settings in the Messenger Admin Tool

To set up or modify the Listener configuration, please go to **Configuration** → **Listeners** in the navigation bar.

Listener Connection

Enter the IP address and port for the Listener connection (Messenger to Listener). The standard port number for this connection is 9000 and 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.

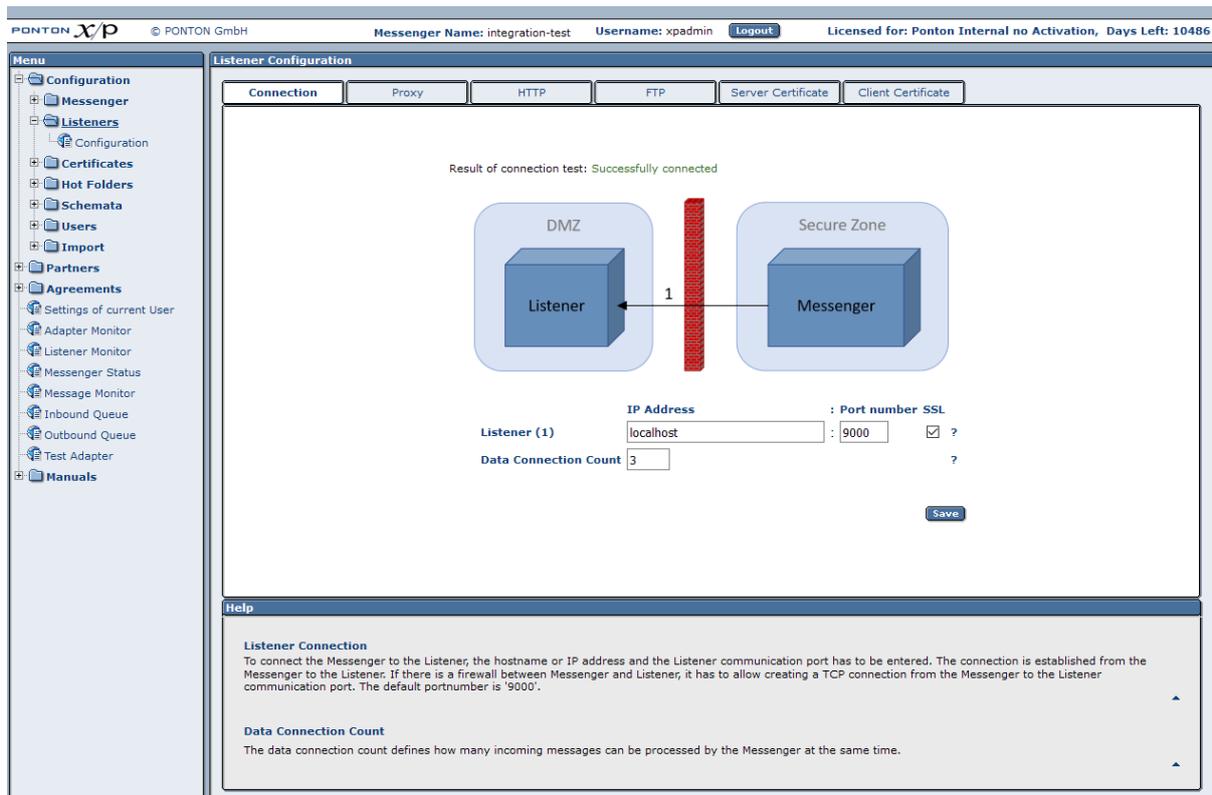
The Listener will only accept connections from known Messenger instances which are listed in the `ListenerConfiguration\config\authorization.txt` File in the Listener Installation.

Please note: The first connection from a Messenger instance to a freshly installed Listener will always be accepted by the Listener !

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.

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 20.



The screenshot displays the 'Listener Configuration' window in the PONTON X/P Messenger application. The interface includes a navigation menu on the left and a main configuration area on the right. The main area is divided into tabs: 'Connection', 'Proxy', 'HTTP', 'FTP', 'Server Certificate', and 'Client Certificate'. The 'Connection' tab is active, showing a diagram of a DMZ containing a 'Listener' and a 'Secure Zone' containing a 'Messenger'. A red vertical bar representing a firewall separates them, with a '1' indicating a connection. Below the diagram, the configuration fields are: 'Listener (1)' with 'IP Address' set to 'localhost' and 'Port number' set to '9000'. The 'Data Connection Count' is set to '3'. There are checkboxes for 'SSL' and '?' next to the port number. A 'Save' button is located at the bottom right of the configuration area. A 'Help' section at the bottom provides details on 'Listener Connection' and 'Data Connection Count'.

Listener Configuration

Result of connection test: Successfully connected

DMZ: Listener

Secure Zone: Messenger

1

Listener (1) IP Address: localhost Port number: 9000 SSL: ?

Data Connection Count: 3 ?

Save

Help

Listener Connection
To connect the Messenger to the Listener, the hostname or IP address and the Listener communication port has to be entered. The connection is established from the Messenger to the Listener. If there is a firewall between Messenger and Listener, it has to allow creating a TCP connection from the Messenger to the Listener communication port. The default portnumber is '9000'.

Data Connection Count
The data connection count defines how many incoming messages can be processed by the Messenger at the same time.

Proxy Settings

With this setting you can enable the use of the Listener as a HTTP proxy server for outbound connections.

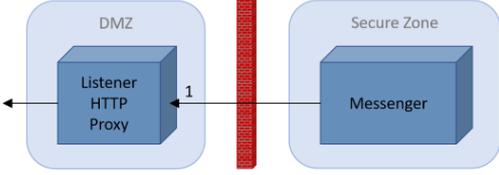
PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10486

Menu

- Configuration
 - Messenger
 - Listeners
 - Configuration
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Listener Configuration

Connection Proxy HTTP FTP Server Certificate Client Certificate



enabled disabled

IP Address : Port number

Proxy (1) * : 13128 ?

Save

Help

Proxy (1)
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.

HTTP Connection Settings

The settings on this tab specify the Listener configuration for incoming HTTP/HTTPS connections.

- HTTP / HTTPS – enables the Listener to handle the relevant protocols.
- Listener (1) – specifies the **IP address** and **port** for incoming connections of the relevant protocol (HTTP or HTTPS).
- 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 on the Client Certificate tab.
- Use partner certificates – specifies that the partner certificates installed in your Messenger's partner configurations will be copied to the Listener configuration and used for authentication of incoming HTTPS connections. This also enables automatic synchronization of partner certificates between Messenger and Listener.
- Max. data size – specifies the maximum size of incoming messages, including the transport envelope. The sender will receive a HTTP error when the message size is too large.

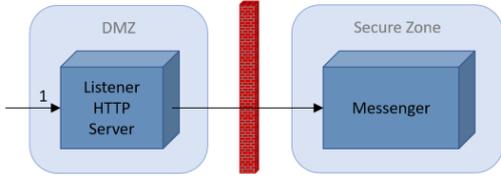
PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10486

Menu

- Configuration
 - Messenger
 - Listeners
 - Configuration
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
 - Manuals

Listener Configuration

Connection Proxy **HTTP** FTP Server Certificate Client Certificate



HTTP

IP Address : Port

Listener (1) * : 26080 ?

HTTPS

IP Address : Port

Listener (1) * : 26843 ?

Client Certificate Check ?

use partner certificates ?

Max. Data Size 4.0 MB ?

Save

Help

Listener
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.

Client Certificate Check
Use SSL client authentication for HTTPS requests. If this option is enabled you need to install a certificate for each communication partner which sends messages via HTTPS to your system.

Use partner certificates
Automatically use the certificates from the configured partners for SSL client authorization.

Max. Data Size

7.1.3. FTP Settings

The common FTP server settings (IP and Port) can be configured on the Config subordinate tab.

Data connection – IP and Port are needed for FTP data transmissions, please make sure that the correct public IP address is provided.

The port-range defines how many simultaneous data transmissions can be executed, because each transmission requires a dedicated port.

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10486

Menu

- Configuration
 - Messenger
 - Listeners
 - Configuration
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
- Manuals

Listener Configuration

Connection Proxy HTTP FTP Server Certificate Client Certificate

Config Logins

FTP enabled

	IP Address	Port
Listener (1)	*	14021 ?
Data Connection (2)	10.0.75.1	15000 - 15010 ?

Save

Help

FTP Listener
The listener IP address and the portnumber is used to connect to your FTP Listener.

FTP Data Connection
The data connection IP address and the portnumber is used to receive messages from communication partners. For any available port use 0.
NOTE: When the FTP Listener has used up all data ports (one per partner doing data transfer), the next partner will have to wait for an available port.

On the Logins tab you can create, delete and edit FTP users and the mapping between FTP user and sender (remote partner).

PONTON X/P © PONTON GmbH Messenger Name: integration-test Username: xpadmin Logout Licensed for: Ponton Internal no Activation, Days Left: 10486

Menu

- Configuration
 - Messenger
 - Listeners
 - Configuration
 - Certificates
 - Hot Folders
 - Schemata
 - Users
 - Import
 - Partners
 - Agreements
 - Settings of current User
 - Adapter Monitor
 - Listener Monitor
 - Messenger Status
 - Message Monitor
 - Inbound Queue
 - Outbound Queue
 - Test Adapter
- Manuals

Listener Configuration

Connection Proxy HTTP FTP Server Certificate Client Certificate

Config Logins

Login Name	Password	Partner	?
<input type="button" value="Create new login"/>			
<input type="button" value="Save"/>			

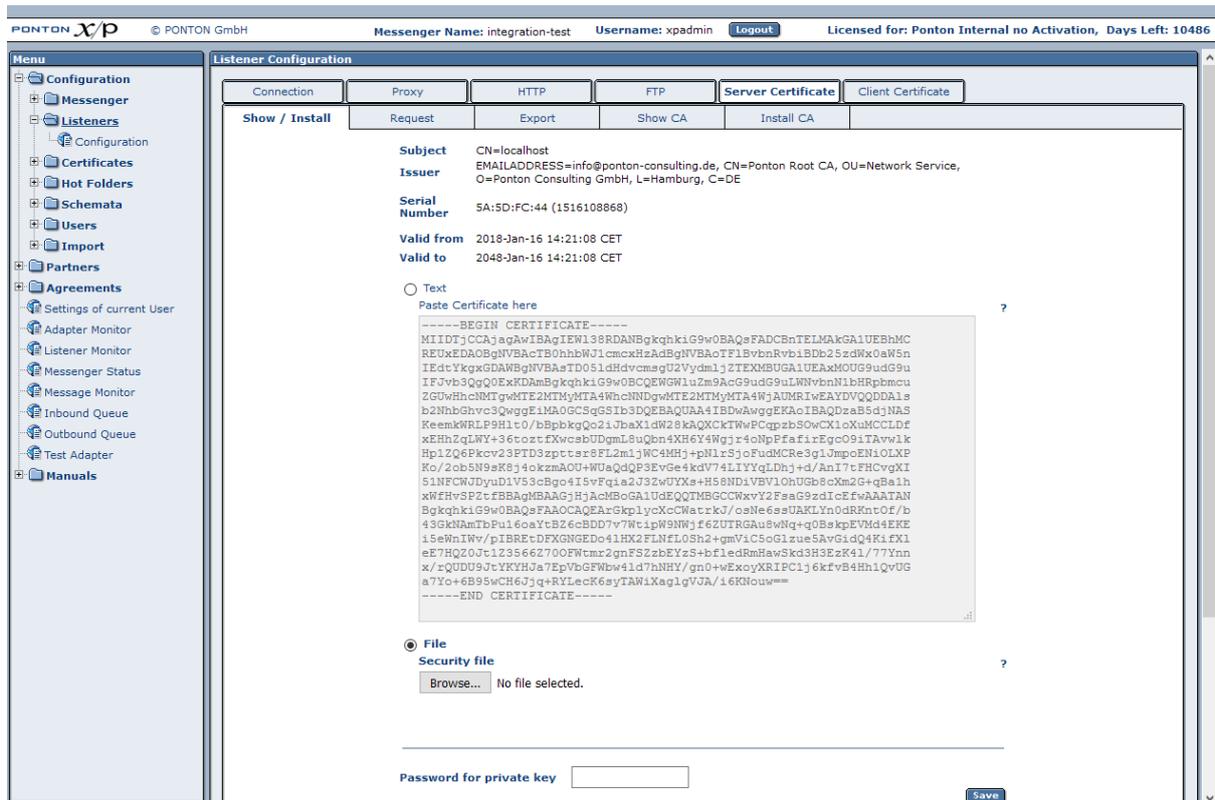
Help

FTP Login
FTP logins allows your partners to connect to your FTP Listener. Every login is linked to one partner profile.

These information (Login Name, Password, IP and PORT) need to be provided to your remote partners to be able to deliver messages successfully to your FTP Listener.

7.1.4. Server Certificate

This tab is for the configuration of your Listener server certificate for HTTPS or FTPS connections.



The screenshot shows the PONTON X/P Messenger interface. The main window is titled "Listener Configuration" and has several tabs: Connection, Proxy, HTTP, FTP, Server Certificate (selected), and Client Certificate. The "Server Certificate" tab is active, showing the following details:

- Subject:** CN=localhost
- Issuer:** EMAILADDRESS=info@ponton-consulting.de, CN=Ponton Root CA, OU=Network Service, O=Ponton Consulting GmbH, L=Hamburg, C=DE
- Serial Number:** 5A:5D:FC:44 (1516108868)
- Valid from:** 2018-Jan-16 14:21:08 CET
- Valid to:** 2048-Jan-16 14:21:08 CET

Below the details, there are two options for installing the certificate:

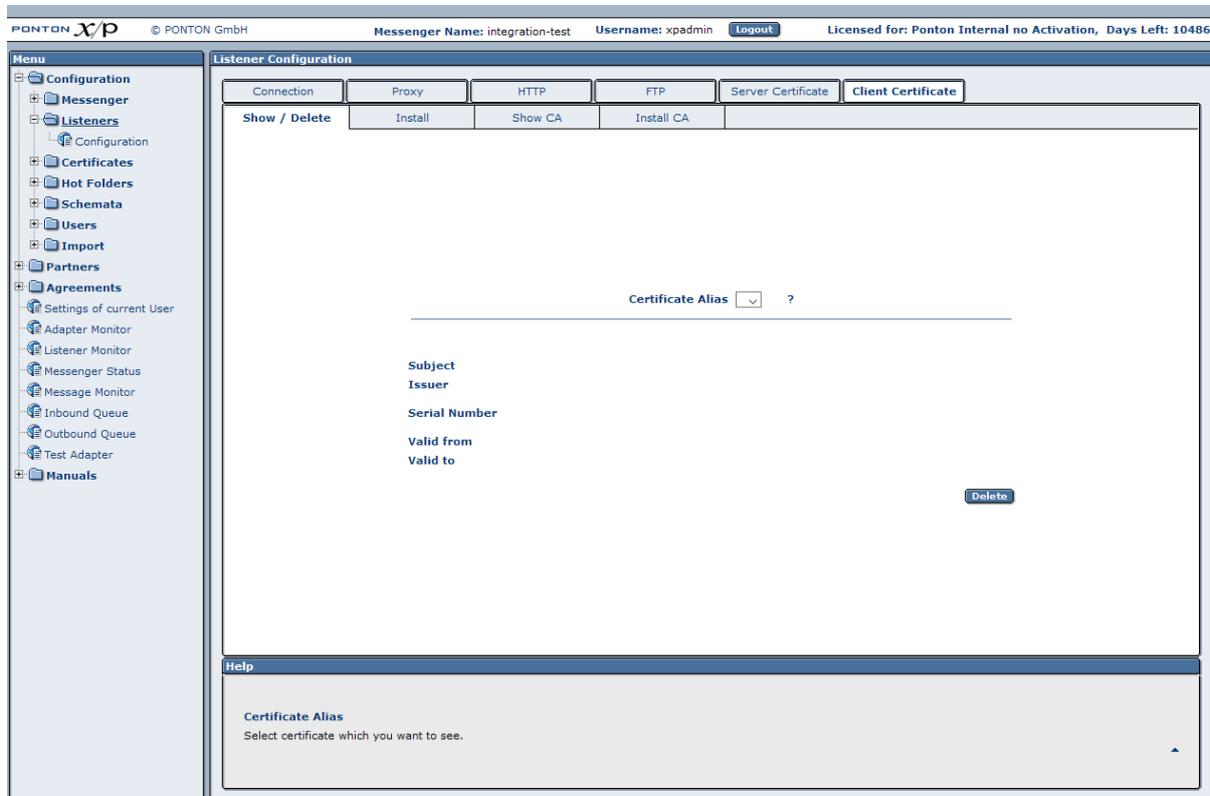
- Text**: Paste Certificate here. A text area contains a long PEM-formatted certificate string starting with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----".
- File**: Security file. A "Browse..." button is present, with the text "No file selected." below it.

At the bottom, there is a field for "Password for private key" and a "Save" button.

The subordinate tabs are used to request and install the server certificate, as well as the CA certificate belonging to the server certificate, if necessary. The PONTON CA certificate is preinstalled, so you will not need to install a CA certificate if you use certificates issued by PONTON.

7.1.5. Client Certificate

This tab is for the configuration of client certificates, which are used for the authentication of HTTPS connections.



The subordinate tabs are used to install (and delete) client certificates as required. For partners using PONTON X/P you can simply import the certificates installed in your Messenger's partner configurations by activating the "Use partner certificates" option on the HTTP tab.

7.1.6. Installing partner certificate on the Listener

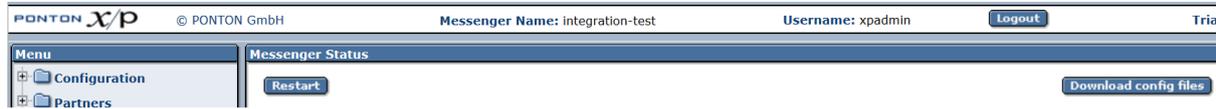
Please take the following steps to install the Partner Certificate of <PARTNER_A> on your listener:

1. In your Messenger Menu please select: Configuration / Listeners / Configuration
2. select the Tab 'Client Certificates' and then select the Tab 'Install'
3. select the option ' Use certificate of Partner ' and finally choose the Partner <PARTNER_A> from the Drop-Down-List available.

By saving these changes this Client Certificate will be installed on the listener machine and then be used for client authentication.

7.2. Set Messenger instance name

Each Messenger instance can be configured to display an instance name to easily identify the system. The name can be a text of 40 characters and it is displayed on the login screen and in the title bar after successful login as shown below:



The name is configured in the configuration file:

launcher/conf/wrapper.conf

```
set.MESSENGER_NAME="MyMessenger"
```

7.3. Messenger Cluster mode

PONTON X/P messenger allows combining multiple Messengers so that they appear as a single instance to external partners or administration users. For more information on this cluster mode, please contact the helpdesk at xp-helpdesk@ponton.de

7.4. Application Monitoring (JMX)

It is possible to monitor PONTON X/P through JMX (for more information on JMX see <http://www.oracle.com/technetwork/java/javase/tech/javamanagement-140525.html>). To enable JMX support you have to set the following system properties:

- `com.sun.management.jmxremote=true`
- `com.sun.management.jmxremote.port=<PORT_NR>`
- `com.sun.management.jmxremote.authenticate=false`
- `com.sun.management.jmxremote.ssl=false`

If you start PONTON X/P as windows service you have to add these properties in the `[installation root]/launcher/conf/wrapper.conf` file like shown below:

```
wrapper.java.additional.10=-Dcom.sun.management.jmxremote=true  
wrapper.java.additional.11=-Dcom.sun.management.jmxremote.port=<PORT_NR>  
wrapper.java.additional.12=-Dcom.sun.management.jmxremote.authenticate=false  
wrapper.java.additional.13=-Dcom.sun.management.jmxremote.ssl=false
```

You have to make sure that the numbering of the wrapper.java.additional lines is sequential. As JMX client you can use the standard JDK tool `jconsole` (for more information see <http://download.oracle.com/javase/8/docs/technotes/guides/management/jconsole.html>) or any other JMX enabled monitoring tool.

7.4.1. Monitoring Partner Connection

To monitor partner connections PONTON X/P provides the PingAll service, which continuously sends EbXML Pings to all communication partners in defined time intervals. On the web GUI go to Configuration → Messenger → Communication where you can enable or disable the service and define the time interval.

The results can be queried through JMX. The JMX ObjectName of the PingAll service is `de.ponton:type=PontonXP,name=PingAll`, which references the MBean `de.pontonconsulting.xmlpipe.adapter.pingall.PingAllThread`.

This MBean contains the follow attributes:

- Enabled – it shows whether the PingAll service is enabled.
- Interval – defined time interval.
- PendingPings – count of currently pending pings.
- PingResultsData – PingResultsTabularType, which contains a list of PingResultCompositeTypes.

A PingResultCompositeType contains the follow attributes:

- SenderId – sender internal id.
- ReceiverId – receiver internal id.
- PingMessageId – message id of the EbXML ping.
- ReplyMessageId – message id of the EbXML reply.
- PingTime – creation time of the EbXML ping.
- ReplyTime – creation time of the EbXML reply.
- Duration – milliseconds between PingTime and ReplyTime.
- Error – flag that indicates if an error occurred.
- Description – contains a description of the messaging result.

7.5. Advanced Database Configuration

Important! Since the Messenger database is used for essential message processing and tracking purposes, you should not experiment with the database configuration on a "live" system. For test and debugging purposes, you are advised to set up a trial system.

7.5.1. Installing other Databases

This section describes the main steps required to install a different database system on the Messenger, for example an Oracle database.

1) Install database driver. Copy the database driver to

[installation root]\lib_ext

Please note that only drivers with the extension *.jar are loaded by PONTON X/P. If the JDBC driver you want to use is a *.zip file, you will have to rename the file to *.jar. For eg. *ojdbc8.jar* for Oracle 12.

2) Create database and tables. PONTON X/P is supplied with SQL scripts for MS SQL Server, MySQL and Oracle. These can be used to create the tables for the Messenger database. If you are using another database, you may need to modify these scripts to work correctly with your database system.

3) Set up database connection. The configuration of database connections is described in the *Messenger Database* section. To connect with a different database, choose a matching database dialect from the dropdown list and enter the Driver Classname and URL in the textboxes.

The entries for the Oracle 12 JDBC driver are:

Driver: oracle.jdbc.driver.OracleDriver

URL: jdbc:oracle:thin:@<host>:<port>:<database>

7.6. XML Schema Configuration

The schema sets available in your Messenger configuration are contained in the following path below the Messenger installation folder:

[installation root]\config\Schemata\

For each schema set there is a configuration file and a subfolder based on the name of the given schema set, for example:

[installation root]\config\Schemata\EFET3.0\

[installation root]\config\Schemata\EFET3.0.xml

In addition, there can be style sheets associated with the schemas in the new schema set. These are stored in a subfolder (based on the name of the given schema set) of the XSL folder, as in:

[installation root]\config\XSL\EFET3.0\

7.6.1. Defining a new Schema Set

The process of adding a new schema set to your Messenger configuration involves the following steps:

- Create a new subfolder within the Schemata folder, using the name of the schema set as the folder name.
- Copy the schemas for the new schema set into this folder.
- Create a new subfolder within the XSL folder, using the name of the schema set as the folder name.
- Copy the style sheets for the new schema set into this folder.
- Create a configuration file according to schemaset.xsd with entries for the schemas contained in the new schema set. If you are not working in a controlled XML editing environment, you may want to create the new configuration file by copying one of the existing XML files and making the necessary changes. The following example shows the structure of configuration entries in this file.

```
<SchemaSet Name="yourSchemaSet">
  <Schema Name="yourSchema" MessageType="yourMsgType" MessageVersion="yourMsgVers"
  Validateable="true" DefaultFileExtension="xml">
    <Namespace>yourNamespace</Namespace>
    <DisplayName>Your Display Name</DisplayName>
    <SchemaFile>your XSD Filename</SchemaFile>
    <XSLFile>your Stylesheet Filename</XSLFile>
    <RootElement>root</RootElement>
  </Schema>
  ...
<SchemaFolder>yourSchemaFolder</SchemaFolder>
<XSLFolder>yourStylesheetFolder</XSLFolder>
</SchemaSet>
```

If the Validateable attribute is set to true, then an XML Schemafile has to exist and need to be referenced in the SchemaFile element.

For identification purposes the Namespace element value and the RootElement values are used.

7.6.2. Extending an existing Schema Set

You can also add a schema to an existing schema set by inserting a `<Schema>` block (just copy and paste one of the existing blocks and modify the configuration as required) in the file. Please ensure that your new schema specification includes correct settings for the attributes of the Schema element:

- Name=This attribute corresponds with the ebXML Schema Location of incoming messages. When an ebXML message is received, the Messenger looks for a schema configuration where the Schema Name attribute matches the Schema Location specified in the ebXML envelope.

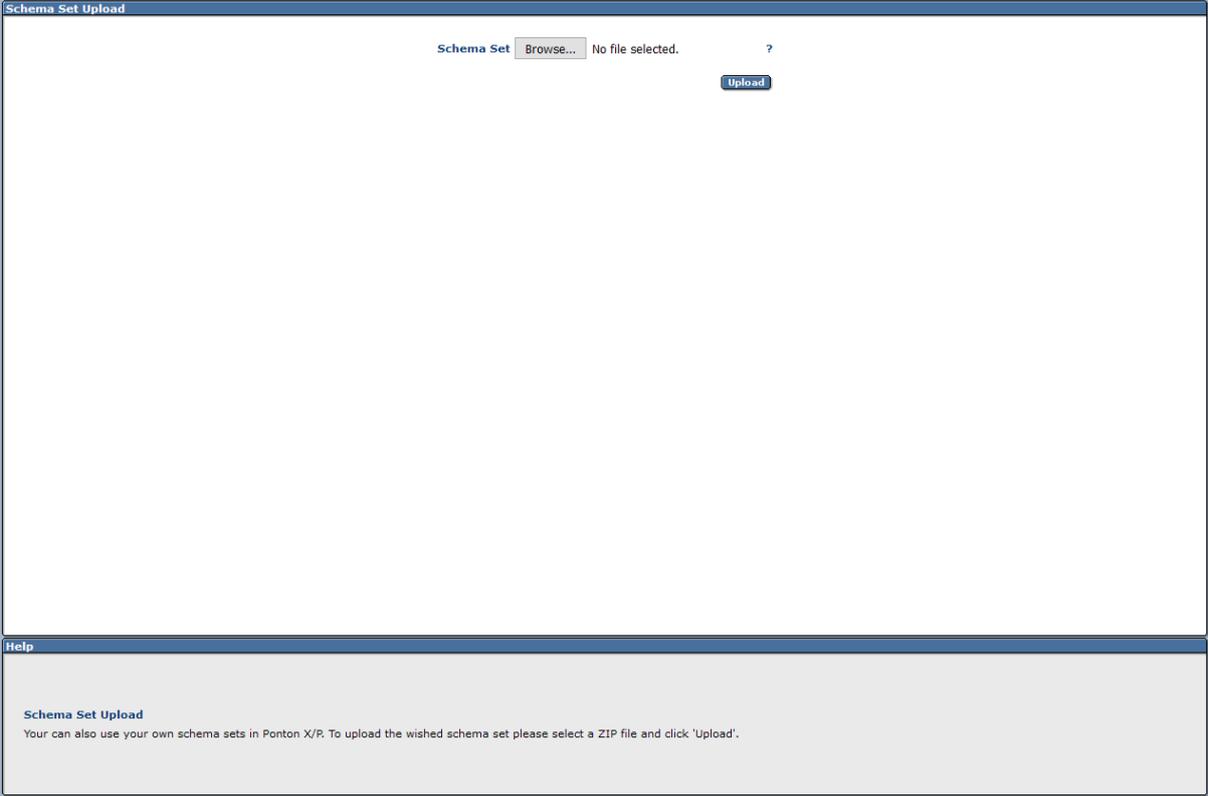
- `MessageType`=This attribute corresponds with the attribute `MessageMetaData/DocumentInfo @MessageName` in the backend envelope of outgoing messages.
- `MessageVersion`=This attribute corresponds with the element `MessageMetaData/DocumentInfo/DTDVersionNumber` in the backend envelope of outgoing messages.

Note: The specification of `MessageType` and `MessageVersion` must be used together for outgoing messages, as they are combined to form an identifier for the message schema.

7.7. Uploading a new Schemaset

A new Schemaset has to be compressed as ZIP archive which might also contain a subfolder with all needed XML schemafiles.

The upload page is found at: Configuration → Schemata → Schema Set Upload



The screenshot shows a web interface for uploading a schema set. At the top, there is a header "Schema Set Upload". Below it, the main area contains a form with the following elements:

- A label "Schema Set" followed by a "Browse..." button and the text "No file selected.".
- A question mark icon to the right of the text.
- An "Upload" button below the form.

At the bottom of the page, there is a "Help" section with the following text:

Schema Set Upload
You can also use your own schema sets in Ponton X/P. To upload the wished schema set please select a ZIP file and click 'Upload'.

7.8. Advanced Message Monitor Configuration

In the configuration directory `/config` there is a file `messagemonitor.xml` which can be used to change the selection and ordering of the Message overview window in the Message Monitor. The default settings are as follows:

```
<?xml version = "1.0" encoding = "UTF-8"?>
<MessageMonitorConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="messagemonitor.xsd">
  <Display>
    <LinesPerPage>6</LinesPerPage>
    <MaxLines>2000</MaxLines>
    <Columns>
      <Column DefaultSortOrder="DESC">RECEPTION_TIME</Column>
      <Column>DB_ID</Column>
      <Column>MESSAGE_ID</Column>
      <Column>MESSAGE_TYPE</Column>
      <Column>SENDER</Column>
      <Column>RECEIVER</Column>
      <Column>DIRECTION</Column>
      <Column>RESULT</Column>
      <Column>TESTFLAG</Column>
      <Column>ACK_RECEIVED</Column>
      <Column>PROTOCOL</Column>
      <Column>LOGINFO</Column>
      <Column>CONVERSATION_ID</Column>
      <Column DefaultSortOrder="DESC">CREATION_TIME</Column>
    </Columns>
  </Display>
  <LogLevel>DEBUG</LogLevel>
  <XSLCaching>true</XSLCaching>
</MessageMonitorConfig>
```

The number of entries displayed per page in the Message Monitor can be set by means of the `LinesPerPage` setting. Particularly if you are using a high resolution screen (with more than 1024 x 768 pixel), you may want to increase the number of lines per page.

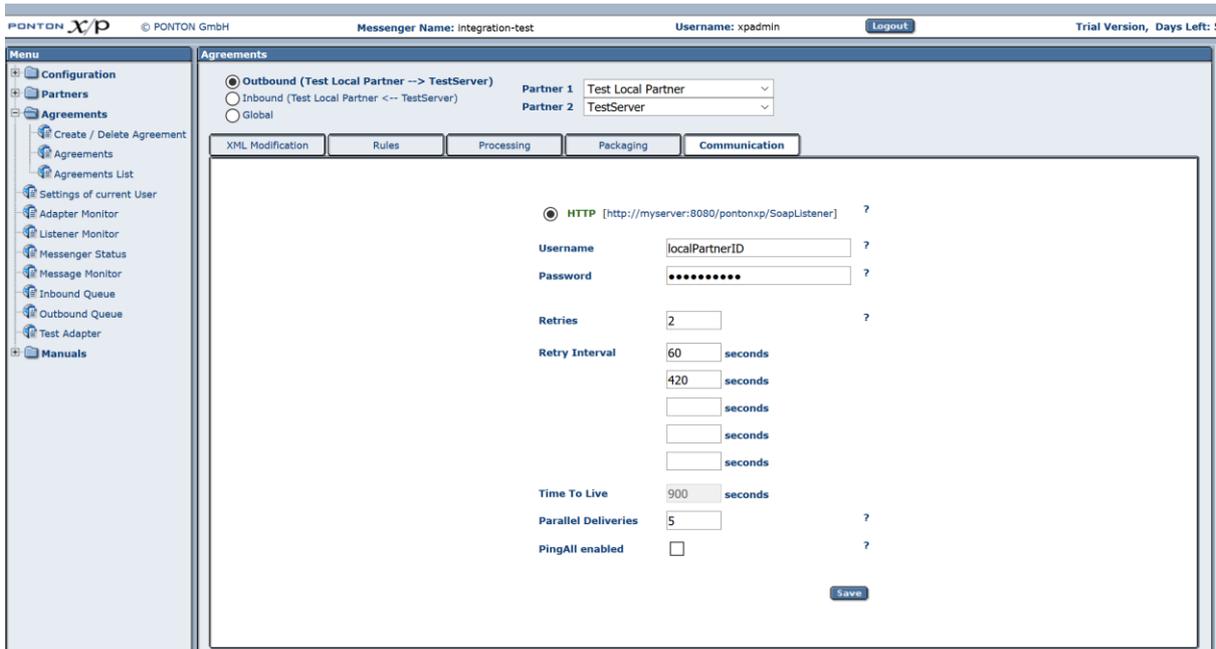
Further, a mapping table defines which database column is to be displayed in which monitor column. The number of columns again depends on the screen resolution.

Finally, if main memory size allows, caching of XSL stylesheet definitions helps accelerating processing speed for XSL transformations.

7.9. Agreement Configuration for Plain Packager

7.9.1. Outbound Configuration

This paragraph describes how to configure an Agreement when sending messages from your Messenger to a receiver without a messaging application by using the Plain Packager.



The screenshot shows the PONTON X/P web interface. The top bar displays "PONTON X/P", "© PONTON GmbH", "Messenger Name: integration-test", "Username: xadmin", and "Logout". The left menu includes "Configuration", "Partners", "Agreements", "Create / Delete Agreement", "Agreements List", "Settings of current User", "Adapter Monitor", "Listener Monitor", "Messenger Status", "Message Monitor", "Inbound Queue", "Outbound Queue", "Test Adapter", and "Manuals". The main area is titled "Agreements" and shows three radio buttons: "Outbound (Test Local Partner --> TestServer)", "Inbound (Test Local Partner <-- TestServer)", and "Global". The "Outbound" option is selected. Below this are dropdown menus for "Partner 1" (Test Local Partner) and "Partner 2" (TestServer). There are five tabs: "XML Modification", "Rules", "Processing", "Packaging", and "Communication". The "Communication" tab is active, showing the following settings:

- HTTP [http://myserver:8080/pontonxp/SoapListener] ?
- Username: localPartnerID ?
- Password: [masked] ?
- Retries: 2 ?
- Retry Interval: 60 seconds, 420 seconds, [empty] seconds, [empty] seconds, [empty] seconds
- Time To Live: 900 seconds
- Parallel Deliveries: 5 ?
- PingAll enabled: ?

A "Save" button is located at the bottom right of the configuration area.

Please note: It is not recommended to use the Plain Packager for communication with messaging software, as all features which are covered by a transport envelope do not exist or are limited, like reliability, security, duplicate control.

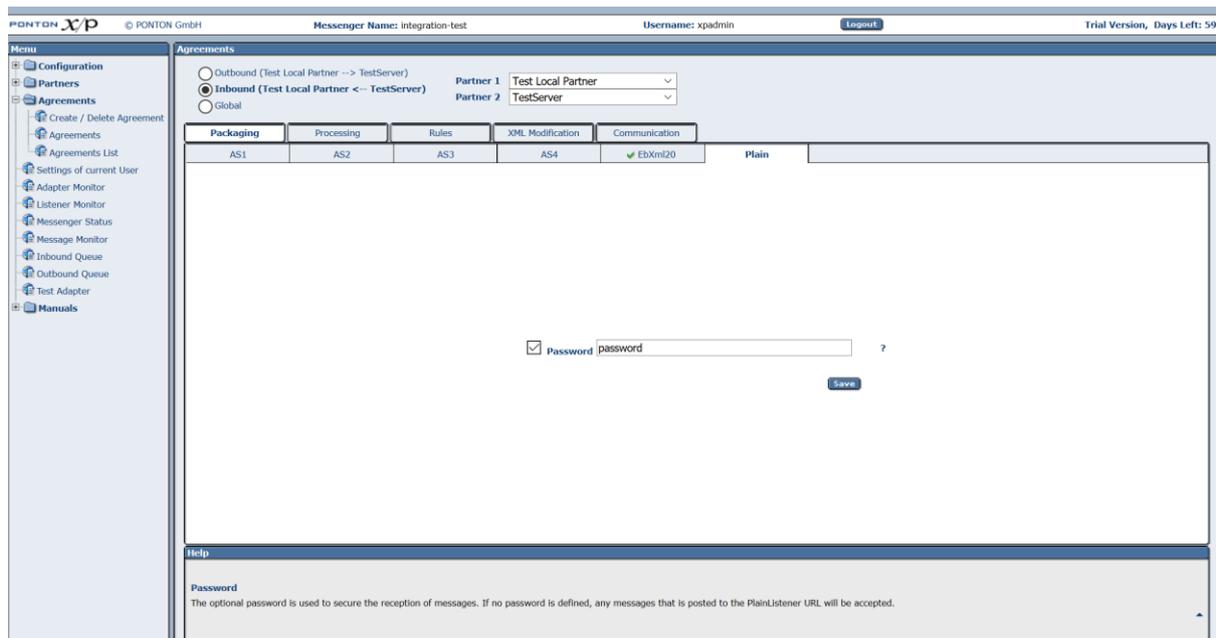
- Communication: If the receiver requires HTTP or FTP authentication, the user and password need to be configured in the outbound communication page
- Packaging: Select the "Plain" tab.
- Processing: Please clarify if your counterparty has any possibilities of processing. Usually you will have to turn off Signing, Encryption and Compression.

The resulting transmission is a HTTP POST or FTP STOR with a pure XML content which is containing the unaltered XML message as it was received by the Messenger from the Adapter.

The communication is successful if the receiver returns a **HTTP 200 result-code** or **FTP 226 result-code**. Any other code will be regarded as a failure

7.9.2. Inbound Configuration

To enable your Messenger to receive pure XML messages without transport envelope, you have to select the Plain Packager on the inbound direction of the Agreement. You can fill in a password that the sender has to transmit to be allowed to send messages. For security reasons it is recommended to specify a password for each Partner Agreement.



Inbound Messages need to be transmitted as HTTP POST to the URL http://YOUR_IP:PORT/pontonxp/PlainListener or FTP STOR to the URL ftp://YOUR_IP:PORT/inbound/plain/PARTNER_ID/FILENAME that you have to setup in the Communication page of the **Partner Configuration**.

It is recommended to select HTTPS or FTPS as protocol to avoid that username and password are transmitted in plain text.

Additionally, the Messenger needs to know who the sender and receiver are. There are two options to provide the Messenger with this information using HTTP:

- The sender transmits HTTP BASIC authentication information with the POST. Username needs to be constructed of receiver id, sender id and a dollar sign as separator. For example: receiver\$sender the password has to match what is configured in the inbound packaging options, if the password is disabled any password is accepted.
- The sender transmits additional HTTP parameters as part of the URL. For example: [http://YOUR_IP:PORT/pontonxp/PlainListener?cpa=receiver\\$sender&pass=password](http://YOUR_IP:PORT/pontonxp/PlainListener?cpa=receiver$sender&pass=password) the password has to match what is configured in the inbound packaging options, if the password is disabled any password is accepted.

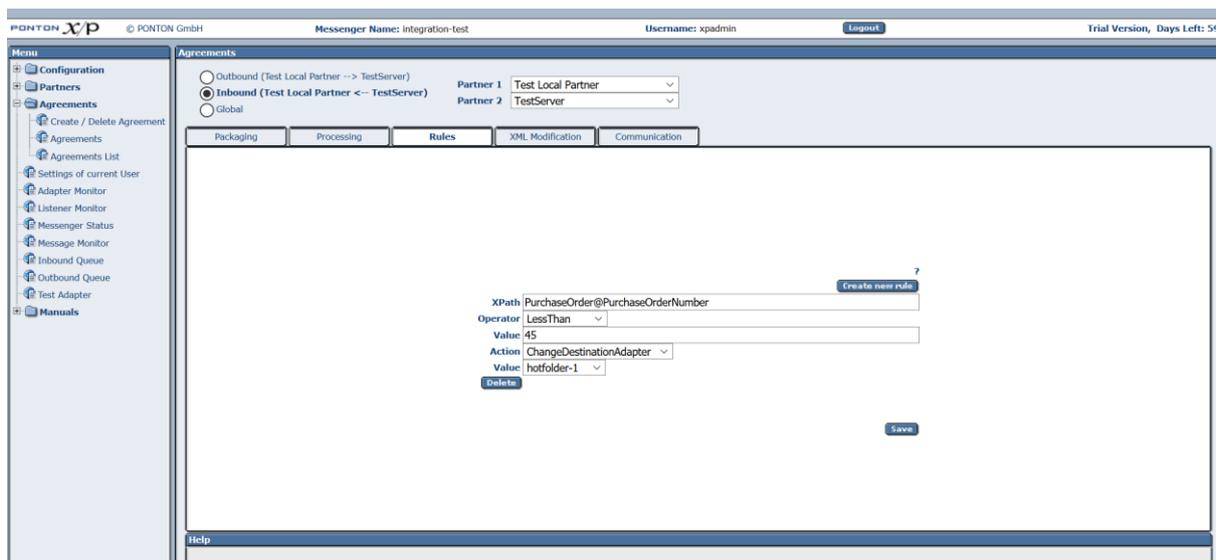
If FTP is selected as transmission protocol, the information of sender and receiver must be transmitted similar to communication via HTTP. The sender will be identified using FTP

authentication information, which can be explicitly set for each agreement or for all agreements, if the authentication information is a part of FTP URL like this:
 ftp://USERNAME:PASSWORD@YOUR_IP:PORT/inbound/plain/PARTNER_ID/FILENAME.
 Association between the FTP user and sender must be configured in your Listener. For details please refer to the FTP Settings section. The receiver will be identified using the last part of the URL. In this case is PARTNER_ID is the identifier of the receiver.

7.10. Content Rules

You can define special rules that determine how messages will be processed based on specified content (within the message or the envelope). The content rules are defined specifically for each partner agreement.

To create a new content rule go to Configuration → Agreements and choose the agreement you want to modify (i.e. the relevant local and remote partner). Then open the Rules tab and click on Create New Rule.



The basic definition of a content rule includes

- XPath – this setting specifies the element or attributes to be checked for a given value or value range.
- Operator – the operator used for comparing values.
- Value – the value to be checked.

In addition to the specification of an element or attribute within the document, it is also possible to use the following reference keys in the XPath field to specify the associated message information:

- **!MessageId** - The Message-ID of the outgoing or incoming message.
- **!ConversationId** - The Conversation-ID of the outgoing or incoming message.
- **!MessageType** – The Message Type as specified in the document schema. Note: The available message types are displayed in the Message Monitor in the Message Type list.
- **!MessageVersion** – This field identifies the schema version. The relevant version IDs can be found in the schema set definition files located under [installation root]\config\Schemata
- **!SchemaSet** – This field identifies the schema set name. The relevant names can be found in the schema set definition files located under [installation root]\config\Schemata
- **!TestFlag** – This flag is set to TRUE for test messages, otherwise it is FALSE.
- **!LogInfo** – This field may contain remarks or any other text. The contents are displayed in the Message Monitor.

For outgoing messages – based on the given agreement – the content rule can be used to trigger a log entry and/or an e-mail notification and furthermore the destination URL can be changed. So it is possible to route certain messages to different servers or URLs.

For incoming messages the content rule can also be used to determine which Adapter is used for message processing.

The action to be taken is based on the Action setting:

- Action – you can select one of the following actions: *Flag*, *EMailNotification*, *ChangeDestinationAdapter* (for incoming messages only) and *ChangeDestinationURL* (for outgoing messages only).

Depending on the selected action, different settings are required:

- For *EMailNotification* – specify the receiver's e-mail address as well as any subject elements to be used. For details on defining subject elements see the *E-mail Notification* section.
- For *ChangeDestinationAdapter* – choose the adapter to be used for message processing. The value field contains a list of the available adapters.
- For *ChangeDestinationURL* – choose the URL to be used for the message. The value field contains all configured URLs for the receiving partner.

Note: The use of *!SenderId* or *!ReceiverId* as filter criteria is no longer supported since these are already specified as the local and remote partners of the relevant agreement. In other words, *content rules are always sender and receiver specific*.

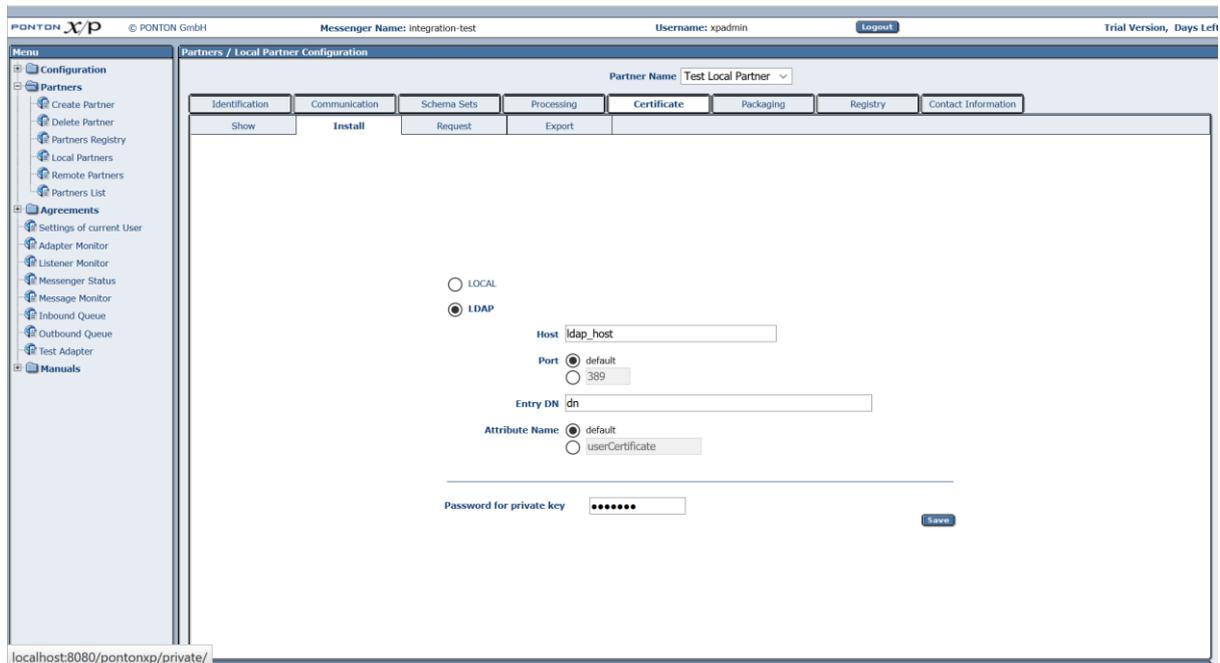
7.11. Partner Certificates

7.11.1. LDAP Certificate Import

If the certificates that should be installed are located on a public LDAP server, it is also possible to directly import the certificates from that server. On the Show/Install Tab, the LDAP radio button has to be clicked to display the LDAP related configuration.

Please consult your LDAP administrator about the needed DN and Attribute settings.

Also note that certificates for remote partners with a LDAP references will also be checked for updates during the regular automatic certificate-update.



The screenshot shows the PONTON X/P web interface. The top navigation bar includes the PONTON logo, version information (© PONTON GmbH), Messenger Name (Integration-test), Username (xadmin), and a Logout button. The main content area is titled 'Partners / Local Partner Configuration' and shows the configuration for 'Test Local Partner'. The 'Certificate' tab is active, and the 'Install' sub-tab is selected. The configuration is set to 'LDAP' (radio button selected). The fields are as follows:

- Host: ldap_host
- Port: default (radio button selected), 389 (radio button unselected)
- Entry DN: dn
- Attribute Name: default (radio button selected), userCertificate (radio button unselected)
- Password for private key: [masked]

A 'Save' button is located at the bottom right of the configuration area. The status bar at the bottom left shows the URL: localhost:8080/pontonxp/private/.

7.12. Data Extraction from XML documents

PONTON X/P is able to populate certain variables with values from the transmitted XML documents. XML XPATH definitions are used to describe where the needed values are found in the documents.

Values from the XML document can be used to set:

- Sender Internal Id
- Receiver Internal Id
- Message Id
- Log Info
- Message Type

- Message Version
- Schema Set
- Test Flag

Please note that mappings will not have an effect for incoming messages if the used B2B Protocol already set the values.

The priority of mappings is:

B2B-Protocol or API » Envelope mapping » Payload Mapping

There is one exception to this rule which is the Log Info mapping where the order is reversed. So if there is a payload mapping defined for Log Info then this will always override any other value.

7.12.1. XPATH Types

There are two types of XPATH available in Ponton X/P:

- Standard W3C XPATH version 1.0
- Ponton subset of XPATH version 1.0

The Ponton subset of XPATH does only support the */* and *@* operators and ignores any namespaces using these characters. This allows very simple expressions especially if documents with multiple namespaces are used. It also allows very fast extraction of content on documents of unlimited size. For most cases this type of XPATH should be sufficient.

Example:

```
/Root2/Header/@Id
```

For other cases the standard W3C XPATH can be used.

Please note that this will always load the full document into memory, so for very large documents this might not be an option.

With standard memory settings a document larger than 5MB is considered to be very large.

Example:

```
/[local-name()='Root1' and namespace-uri()='http://p.de/m.xsd']/[local-name()='Header' and namespace-uri()='http://p.de/m.xsd']/@Id
```

7.12.2. Envelope Mapping

Envelope definitions describe global XML structures that are wrapped around message documents. Such envelopes usually contain messaging specific meta-data.

For each Envelope type there needs to be one xml file in the folder [*installation root*]/config/Envelopes/. These xml files need to conform to the envelope_mapping.xsd also found in the same folder.

All mapping definitions for envelopes are optional except for the "PayloadXPath" as this describes where the actual XML messages are embedded in the envelope. The XPath for this always has to end with a star.

Code Block 6 Example

```
<EnvelopeMapping Name="env_ponton" RootElement="pontonEnvelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="envelope_mapping.xsd">
  <SchemaFile>env_p/pontonEnvelope.xsd</SchemaFile>
  <Namespace>http://ponton.de/env_ponton/v1r00</Namespace>
  <Mapping XPathType="Ponton">
    <PayloadXPath>/pontonEnvelope/Payload/*</PayloadXPath>
    <MessageIdXPath>/pontonEnvelope/ID</MessageIdXPath>
    <LogInfoXPath>/pontonEnvelope/LogInfo</LogInfoXPath>
  </Mapping>
</EnvelopeMapping>
```

7.12.3. Payload Mapping

The mapping of content specific to message types is defined in the schema-set definition files found in the folder [*installation root*]/config/Schemata/.

These xml files need to be conform with the schemaset.xsd found in the same folder. The EnvelopeMapping section is optional and can be defined individually for each message type, for eg.:

Code Block 7 Example

```
<Schema Name="mapping2.xsd" MessageType="PurchaseOrder" MessageVersion="2.0">
  <Namespace>http://ponton.de/mapping2.xsd</Namespace>
  <DisplayName>PurchaseOrder</DisplayName>
  <RootElement>PurchaseOrder</RootElement>
  <SchemaFile>mapping2.xsd</SchemaFile>
  <XSLFile/>
  <EnvelopeMapping XPathType="Ponton">
    <LocalPartyIdXPath>/PurchaseOrder/Header/Sender</LocalPartyIdXPath>
    <RemotePartyIdXPath>/PurchaseOrder/Header/Receiver</RemotePartyIdXPath>
    <MessageIdXPath>/PurchaseOrder/Header/@Id</MessageIdXPath>
    <LogInfoXPath>/PurchaseOrder/Header/LogInfo</LogInfoXPath>
  </EnvelopeMapping>
</Schema>
```

8. Troubleshooting

8.1. Locating Inconsistencies in a Partner Agreement

Ponton X/P offers a convenient feature for locating inconsistencies between the settings in a partner agreement and the settings in the relevant partner configurations. If a setting is found to be inconsistent the Admin Tool will display the following messages and markers:

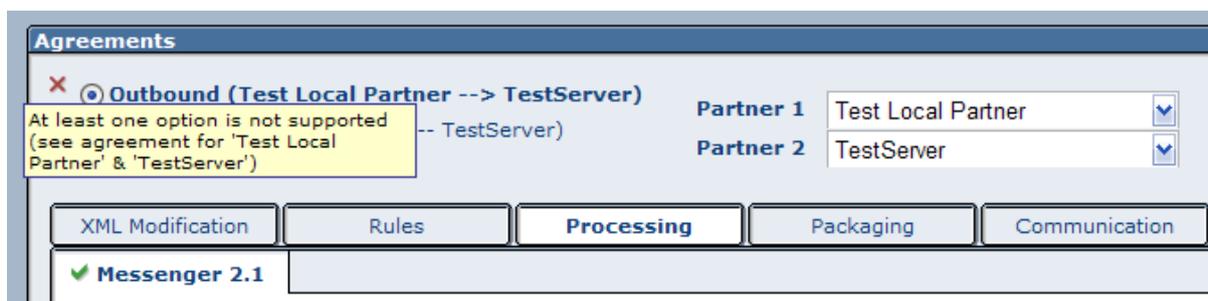
- On the **Messenger Status** page, the inconsistent settings are shown in the **Events** list. The corresponding entries indicate which partner agreement is affected, for example:

Events:

Time	Component	Description	
2007-07-04 15:00:23 CEST	Agreement (Receive: Processing)	At least one option is not supported (see agreement for 'Test Local Partner' & 'TestServer')	
2007-07-04 15:00:23 CEST	Agreement (Send: Processing)	At least one option is not supported (see agreement for 'Test Local Partner' & 'TestServer')	

Hint: To call up the relevant configuration page for the given agreement you can simply click on the description.

- Within the agreement configuration, the presence of an incorrect or inconsistent setting is marked by a small red **x** in the upper left corner (next to the Outbound – Inbound – Global selection). If you point your mouse at the small **x** marker you will see a tool tip indicating that an inconsistency has been found, for example:



- On the specific page in the agreement configuration where the incorrect or inconsistent setting is located, the label for the relevant setting is colored red, for example:

Agreements

Outbound (Test Local Partner --> TestServer)
Partner 1: Test Local Partner
Partner 2: TestServer

Inbound (Test Local Partner <-- TestServer)

Global

XML Modification
Rules
Processing
Packaging
Communication

✓ **Messenger 2.1**

Signing
SHA1withRSA

C This pipeline option is not supported by the both partners 'Test Local Partner' & 'TestServer'.

Encryption
DES_EDE3_CBC

Certificate
default
?

Compression
Zlib
?

Validation
?

?

By pointing your mouse at the label you can call up a tool tip with further information. If you disable the relevant setting and then save the agreement, you will see that the option is removed from the agreement page, since it is no longer supported by at least one of the partners.

8.2. Port Configuration

The Messenger's standard configuration uses port 8080 for HTTP connections and port 8443 for secure (HTTPS) connections. If those ports are already in use or they are not allowed due to firewall policies, then it is necessary to adjust the default ports.

This section describes how to set up the messenger to use a non-default port configuration.

8.2.1. HTTP Settings

The port setting for the Messenger's HTTP and HTTPS connections are stored in the configuration file server.xml:

[installation root]\config\server.xml

This file defines the connections (Connectors) for the Messenger like this:

Code Block 8 Connector configuration

```
<Connector id="1">
  <Address>*</Address>
  <Port>8443</Port>
  ...
</Connector>
The standard settings for the Messenger ports are
HTTP port: 8080 for Adapters
HTTPS port: 8443 for GUI
Shutdown port :7626
```

To modify your connections, you will need to enter the relevant port numbers indicated above as *Port*.

8.3. Identification of Message-Type

When an inbound message is processed it is important that the message can be recognized as a specific message type.

The Messenger is able to use meta information from the message content for identification purposes. Any of the following data is used in this process:

- DocType definition
- Schema location definition
- Schema-Namespace
- Root-Element name

If none of this was found, then it is not possible to validate the message against an XML Schema.

9. Supported Crypto Algorithms

9.1. EbXML20 Packager

The EbXML20 packager supports the following security algorithms:

Packager Option	Algorithm
XmlSignature	http://www.w3.org/2000/09/xmlsig#rsa-sha1

9.2. AS1/AS2/AS3 Packager

The AS1/AS2/AS3 packager supports the following security algorithms:

Packager Option	Algorithm
MD5 signed	MD5withRSA
SHA-1 signed	SHA1withRSA
SHA-1/PSS signed	SHA1withRSAandMGF1
SHA-224 signed	SHA224withRSA
SHA-224/PSS signed	SHA224withRSAandMGF1
SHA-256 signed	SHA256withRSA
SHA-256/PSS signed	SHA256withRSAandMGF1
SHA-256/ECDSA signed	SHA256withECDSA
SHA-384 signed	SHA384withRSA
SHA-384/PSS signed	SHA384withRSAandMGF1
SHA-384/ECDSA signed	SHA384withECDSA
SHA-512 signed	SHA512withRSA
SHA-512/PSS signed	SHA512withRSAandMGF1
SHA-512/ECDSA signed	SHA512withECDSA
AES128_CBC	AES128_CBC
AES128_CBC/OAEP_SHA1	AES128_CBC_RSA_OAEP_SHA1_MGF1
AES128_CBC/OAEP_SHA256	AES128_CBC_RSA_OAEP_SHA256_MGF1
AES128_CBC/OAEP_SHA512	AES128_CBC_RSA_OAEP_SHA512_MGF1
AES128_GCM	AES128_GCM
AES128_GCM/OAEP_SHA256	AES128_GCM_RSA_OAEP_SHA256_MGF1
AES128_GCM/OAEP_SHA512	AES128_GCM_RSA_OAEP_SHA512_MGF1
AES128_GCM/ECDH_SHA224	AES128_GCM/ECDH_SHA224
AES128_GCM/ECDH_SHA256	AES128_GCM/ECDH_SHA256

Packager Option	Algorithm
AES128_GCM/ECDH_SHA512	AES128_GCM/ECDH_SHA512
AES192_CBC	AES192_CBC
AES192_CBC/OAEP_SHA1	AES192_CBC_RSA_OAEP_SHA1_MGF1
AES192_CBC/OAEP_SHA256	AES192_CBC_RSA_OAEP_SHA256_MGF1
AES192_CBC/OAEP_SHA512	AES192_CBC_RSA_OAEP_SHA512_MGF1
AES192_GCM	AES192_GCM
AES192_GCM/OAEP_SHA256	AES192_GCM_RSA_OAEP_SHA256_MGF1
AES192_GCM/OAEP_SHA512	AES192_GCM_RSA_OAEP_SHA512_MGF1
AES192_GCM/ECDH_SHA224	AES192_GCM/ECDH_SHA224
AES192_GCM/ECDH_SHA256	AES192_GCM/ECDH_SHA256
AES192_GCM/ECDH_SHA512	AES192_GCM/ECDH_SHA512
AES256_CBC	AES256_CBC
AES256_CBC/OAEP_SHA1	AES256_CBC_RSA_OAEP_SHA1_MGF1
AES256_CBC/OAEP_SHA256	AES256_CBC_RSA_OAEP_SHA256_MGF1
AES256_CBC/OAEP_SHA512	AES256_CBC_RSA_OAEP_SHA512_MGF1
AES256_GCM	AES256_GCM
AES256_GCM/OAEP_SHA256	AES256_GCM_RSA_OAEP_SHA256_MGF1
AES256_GCM/OAEP_SHA512	AES256_GCM_RSA_OAEP_SHA512_MGF1
AES256_GCM/ECDH_SHA224	AES256_GCM/ECDH_SHA224
AES256_GCM/ECDH_SHA256	AES256_GCM/ECDH_SHA256
AES256_GCM/ECDH_SHA512	AES256_GCM/ECDH_SHA512
DES_EDE3_CBC	DES_EDE3_CBC
DES_EDE3_CBC/OAEP_SHA1	DES_EDE3_CBC_RSA_OAEP_SHA1_MGF1

9.3. AS4 Packager

The AS4 packager supports the following security algorithms:

Packager Option	Algorithm
rsa-sha1	http://www.w3.org/2000/09/xmldsig#rsa-sha1
rsa-sha256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
rsa-sha512	http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
aes128-cbc	http://www.w3.org/2001/04/xmlenc#aes128-cbc
aes128-gcm	http://www.w3.org/2009/xmlenc11#aes128-gcm
aes256-cbc	http://www.w3.org/2001/04/xmlenc#aes256-cbc
aes256-gcm	http://www.w3.org/2009/xmlenc11#aes256-gcm

Packager Option	Algorithm
tripleDES-cbc	http://www.w3.org/2001/04/xmlenc#tripleDES-cbc

9.4. Messenger 2.1 Payload Processor

The following security algorithms are supported:

Processing Option	Algorithm
MD5withRSA	MD5withRSA
SHA1withRSA	SHA1withRSA
SHA512withRSA	SHA512withRSA
SMIME-SHA1	SHA1withRSA
SMIME-SHA512	SHA512withRSA
AES256_CBC	AES256_CBC
DES_DES3_CBC	DES_DES3_CBC
SMIME-AES256_CBC	AES256_CBC
SMIME-DES_DES3_CBC	DES_DES3_CBC

9.5. SSL/TLS

The following protocols/ciphers are supported:

Supported Protocols
SSLv2Hello
SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Supported SSL/TLS Ciphers
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

Supported SSL/TLS Ciphers

TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256

Supported SSL/TLS Ciphers

TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

PONTON GmbH
Dorotheenstraße 64
GERMANY 22301 Hamburg
Web: <http://www.ponton.de>