

PAS-X MES

System Requirements

System manual





PAS-X MES
System manual

Körber Pharma Software
PAS-X MES Standard
Valid as of software version V3.3.2/00
Document version 1.3
Modification date: 25 May 2023

Company, product and service names may be trademarks or service marks of their respective owners.

Körber Pharma Software GmbH
Wulf-Werum-Str. 3 · 21337 Lüneburg · Germany
T +49 4131 8900 0 · info.pasx@koerber.com · koerber-pharma.com

Table of contents

1	General.....	7
1.1	Purpose.....	7
1.2	Target audience.....	7
1.3	Symbols and typographical conventions.....	7
1.4	Miscellaneous.....	9
2	Abbreviations / Definition of Terms.....	10
3	Introduction to the MES Infrastructure.....	14
3.1	Typical PAS-X MES Infrastructure.....	14
3.1.1	DMZ 3/4 (Interfacing Zone).....	14
3.1.2	Level 3 (Manufacturing Operations Management).....	15
3.1.3	DMZ 2/3 (Interfacing Zone).....	16
3.1.4	Corporate Level.....	16
3.1.5	PAS-X Client Options.....	17
3.2	PAS-X Optional Components.....	17
3.2.1	PDF/A conversion.....	17
3.2.2	PAS-X Monitoring Service.....	17
3.2.3	PAS-X Authentication Adapter.....	18
3.2.4	Deployment registry.....	18
4	Requirements.....	19
4.1	Container Orchestration Platform.....	19
4.1.1	Docker Swarm.....	19
4.1.2	Kubernetes.....	31
4.1.3	PAS-X System Services.....	39
4.2	Client Peripherals.....	49
4.2.1	Client Screen Size.....	49
4.2.2	Barcode Scanners.....	49
4.3	Common Unix Printing System (CUPS).....	49
4.3.1	Supported printers.....	49
4.3.2	Adding Printers to CUPS.....	50
4.3.3	Configure PAS-X Printing Service to use CUPS.....	51
4.3.4	Configure PAS-X Printing Service.....	51
4.3.5	CUPS Security.....	51
4.4	Database.....	51
4.4.1	Oracle software requirements.....	52
4.4.2	Oracle database requirements.....	52

4.4.3	Oracle user requirements	55
4.4.4	PostgreSQL software requirements	56
4.4.5	PostgreSQL database requirements	56
4.4.6	PostgreSQL database prerequisites	59
4.5	ERP Integration	61
4.5.1	XML IDoc	61
4.5.2	SAP RFC	61
4.6	Fonts	61
4.7	Operating System	61
4.8	Password Encryption	62
4.8.1	Restricted characters for configuration property values	62
4.9	PAS-X Client	62
4.9.1	Java Runtime Environment (JRE)	63
4.9.2	Web Start (IcedTea-Web)	63
4.9.3	Web Browser	67
4.9.4	Citrix Terminal	72
4.9.5	Encrypted Client Communication	72
4.10	PDF/A conversion / Ghostscript	72
4.11	Time Zone	72
5	Appendix	74
5.1	Supporting Infrastructure Components	74
5.2	Systems Sizing Introduction	74
5.3	Availability Options	74
5.4	Production Network	74
5.5	Virtualization Statement	75
5.6	Recommended Monitoring Spots for PAS-X Systems	75
5.7	Network Communication	76
5.7.1	Network Ports for Docker Swarm	76
5.7.2	Network Ports for Kubernetes	82
5.7.3	Citrix Ports	84
5.8	PAS-X runtime configuration	86
5.8.1	Client	86
5.8.2	Server	86
5.8.3	Platform Releases	87

Document history

Version	Date	Name	Change
1.0	19 Aug 2022	C. Dröscher	Initial document for software version PAS-X MES V3.3.2/00.
1.0	19 Aug 2022	A. Kröger	Updated sections "PAS-X runtime configuration / Server" and "PDF/A conversion / Ghostscript" regarding Ghostscript version.
1.0	07 Oct 2022	K. Hinz	Updated section "Service users" regarding usage of ssh socket connection for traefik.
1.0	07 Oct 2022	K. Hinz	Updated section 'Docker Remote API Access' regarding a secure API access over ssh.
1.0	02 Nov 2022	G. Kirck	Updated section "Password encryption", refer to "System Manager" system manual.
1.0	21 Dec 2022	G. Kirck	Added section "RabbitMQ node labels" and updated section "Host bound PAS-X Services" regarding RabbitMQ deployment and requirements in the Swarm configuration.
1.0	23 Jan 2023	N. Haffke	Editorial changes.
1.0	09 Feb 2023	C. Friedrich	Updated section "PAS-X runtime configuration": Corrected browser & XenApp version for client runtime and Helm & kubectl version for server runtime.
1.0	23 Feb 2023	T. Burlatis	Updated section "PAS-X runtime configuration": Corrected browser version. Corrected PostgreSQL requirements.
1.0	24 Feb 2023	B. Tiernan	Editorial changes.
1.1	27 Feb 2023	T. Burlatis	Corrected Kubectl version.
1.2	11 Apr 2023	T. Burlatis	Updated section "PAS-X runtime configuration": allow applying Citrix CU packages.
1.3	25 May 2023	T. Burlatis	Updated section "PAS-X runtime configuration": added Bash V5 as requirement for deployment host.

Document Creation and Review

Creation and review of this document is typically a joint activity performed by several project team members. The signature confirming creation and review of this document indicates that it has been created and reviewed by the person signing.

It is confirmed that the content of this document fits the purpose described in the respective "Purpose" section in the document.

It is also confirmed that this document is created in a manner that an administrator is able to understand it.

Created and reviewed by

Name / date / signature

Document Review and Approval

Review and approval signatures for this document act as confirmation by the person signing that this document has been created in the way indicated above.


Reviewed and approved by

Name / date / signature

1 General

1.1 Purpose

This section describes the requirements for systems utilizing PAS-X.

-  The hardware structure of PAS-X systems varies:
- from complete systems on a single computer, e.g. for demo systems
 - to distributed system components on several computers (productive systems).

The mentioned system requirements do NOT include requirements for redundant hardware; this means that **requirements for systems employing redundancy concepts are not considered in this document**.

It is assumed that ONLY the PAS-X **productive** system runs on the hardware. **Additional loads caused by other systems**, such as testing and/or training systems running on the same hardware **are not considered in this document**. It is common to have the following systems installed at the customer:






- Development or sandbox system to e.g. perform testing of a prototype
- Training system to train end users, e.g. operators or supervisors
- Qualification system used for validation
- Productive system




1.2 Target audience

This document is aimed for administrators. Prerequisites:

- Technical knowledge relating to the system infrastructure.
- Good command of the functions of the PAS-X user interface.

1.3 Symbols and typographical conventions

Symbol	Description / Example
	Indicates important information for the proper use of the software. Example:  All functions are protected by user rights. If you do not have the respective right, the appropriate button is disabled.
	Indicates useful information designed to make working with the software easier. Example:  To display the navigator permanently, in the upper right corner of the navigator, click: 

Symbol	Description / Example
	<p>Indicates notes that, if not observed, can lead to a loss of data or put the software's support of the process at risk. Example:</p> <p> Deleting ERP locations can cause inconsistencies in the WMS data. Hence, only administrators can delete ERP locations. Before you delete an ERP location, make sure that it is not assigned to WMS locations.</p>
	Indicates information quoted from an external source, e.g. from a website.
✓	Indicates a requirement that must be met before you can complete the corresponding tasks.
1. 2. 3.	<p>Indicates tasks you have to complete. The tasks must be completed in the specified order. Example:</p> <ol style="list-style-type: none"> 1. Open the desired dialog. 2. In the menu bar, click: File > New. 3. In the detail view: Enter the required data. <p>This excludes tasks that depend on a condition. If the condition is not met, skip this task and continue with the next one. Example:</p> <ol style="list-style-type: none"> 1. If the MBR is not in edit mode, in the icon bar, click: Edit. 2. Select the basic operation in which you want to edit a material.
– or –	<p>Indicates alternative tasks you can complete. Example:</p> <ol style="list-style-type: none"> 1. Click Ok. <p>– or –</p> <p>On the keyboard, press [Enter].</p>
►	<p>Indicates the result of a task or a series of tasks. Example:</p> <p>► The filter is deactivated. All entries are displayed.</p>
Bold font	<p>Indicates fixed terms and texts, e.g. buttons or fields in the application window. Examples:</p> <ul style="list-style-type: none"> • Click: Ok. • In the Material no. field: Select a value.
<i>Italic font</i>	<p>Indicates messages and information displayed in the application window or data to be selected or entered by the user. Examples:</p> <ul style="list-style-type: none"> • The message <i>Failed to save your data</i> is displayed. • Enter the value <i>HB125</i>. • The equipment is set to status <i>Allocated</i>.

Symbol	Description / Example
Blue font	<p>Indicates cross-references which can be clicked for further information. Example: See section: "Dialog" title.</p> <p>Also indicates cross-references to an external source of information, e.g. a specific web address. Example: For further information see: www.koerber-pharma.com.</p>
Menu > Menu item > ...	<p>Indicates a navigator or menu path via which you can open a dialog or execute a function. Examples:</p> <ul style="list-style-type: none"> • In the navigator, select: Master Data > Material Master Data > Material. • In the menu bar, click: Help > About.
"Quotation marks"	<p>Indicates emphasis, e.g. additional highlighting of terms in the application window or specific terms used in this documentation. Example:</p> <ul style="list-style-type: none"> • This documentation uses the terms "application window", "work areas", and "dialog".
[Key]	<p>Indicates a key on the keyboard. Examples:</p> <ul style="list-style-type: none"> • On the keyboard, press [Enter]. • To open a pop-up dialog to display the shortcuts for keyboard operation, press [CTRL]+[ALT]+[L].

1.4 Miscellaneous

The dialogs and their content in your installation may differ slightly from the examples and screenshots in this document due to configuration and parameterization.

In addition, corporate design elements may look different in your application, e.g. company and product logos. Also dialog icons may look different, but are placed at the same position in the dialog.

To ensure readability, the use of gender-neutral phrasing may sometimes be omitted. However, the text is meant to always address all genders.

2 Abbreviations / Definition of Terms

Abbreviation / Term	Description
ADDS	Active Directory Domain Services; technology created by Microsoft that provides a variety of network services to centrally configure and administer system, user and application settings.
AMQP	Advanced Message Queuing Protocol
AUDA	PAS-X Authentication Adapter. The service that connects to external systems which implement the external authentication interface (e.g., for authentication via card readers).
BPS	Background Process Server
BRR	Batch Record Report
CA	Certification Authority
CCU	Concurrent Users; total number of people using a resource (application, file, etc.) at the same time
Configuration Service	Service that provides a web UI to dynamically configure all other services.
CS	Central Server; PAS-X Central Service, formerly known as Application Server
CTX	Citrix Server
CUPS	Common Unix Printing System
DBA	Database Administrator
DNS	Domain Name System; hierarchical naming system for computers, services, or any resource participating in the Internet
DNSRR	DNS Round Robin, a technique of load balancing multiple service hosts
DS	Deployment Server
ERP	Enterprise Resource Planning; SAP R/3 is an example for an ERP system
ESR	Extended Support Release
FAT	Factory Acceptance Test

Abbreviation / Term	Description
Firewall	System to block unauthorized access while permitting authorized communications
GPL	General Public License
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDoc	Intermediate Document, a standard data structure used to transfer data between SAP system applications and external systems.
IPP	Internet Printing Protocol
IS	Infrastructure Server
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
JVM	Java Virtual Machine
K8s	Kubernetes ("K" followed by 8 letters "ubernete" followed by "s")
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol; application protocol for querying and modifying directory services running over TCP/IP
Message Monitoring Service (MeMo)	Service that provides a web view for failed messages on the RabbitMQ.
MSI	Message Based Shop Floor Integration
NFS	Network File System
NTP	Network Time Protocol
OPC	Open Platform Communications
ORA	Oracle Database

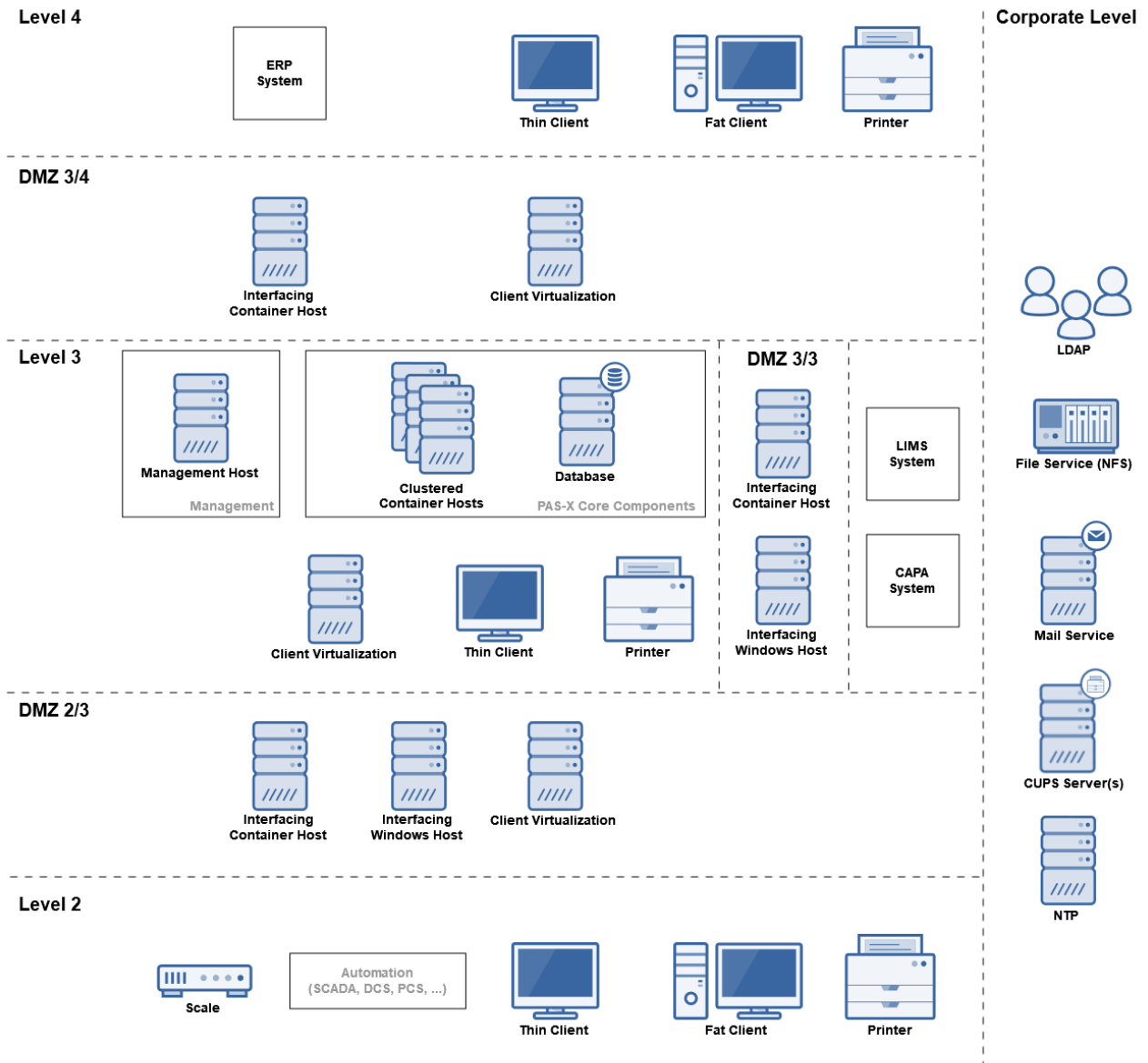
Abbreviation / Term	Description
Oracle Data Guard	Extension to the Oracle RDBMS; aids in establishing and maintaining secondary "standby databases" as alternative/supplementary repositories to production "primary databases".
Oracle Fail Safe	Software option that works with Microsoft Cluster Server (MSCS) to provide high availability for applications and single-instance databases running on Microsoft clusters.
Oracle RAC	Oracle Real Application Cluster; software created by Oracle for clustering and to achieve high availability in Oracle database environments. It allows two or more computers (each with an instance (=multiple-instances)) to concurrently access a single database.
PCS	Process Control System; comprehensive term for DCS/SCADA/PLC
PDF	Portable Document Format
PVC	Persistent Volume Claims
RabbitMQ	Message bus that handles communication between services.
RAID	Redundant Array of Independent Disks; term for data storage systems to increase data reliability or increase input/output performance
RDBMS	Relational Database Management System
RFC	Remote Function Call e.g., SAP RFC
RDP	Remote Desktop Protocol; protocol to provide a graphical interface to connect to another computer over a network connection.
SAN	Storage Area Network; a unit of several external hard disks acting as a local storage
SMB	Server Message Block protocol; used for printer and file sharing on Microsoft Windows Platforms
SSL	Secure Sockets Layer
SUP	Supervision
Terminal Server	A computer to provide a Windows (or Linux) desktop to multiple user terminals
TLS	Transport Layer Security

Abbreviation / Term	Description
UI	User Interface
UPS	Uninterruptible Power Supply
UTC	Time zone name of Coordinated Universal Time
VM	Virtual Machine; simulated instance of a computer
WEI	Werum External Interface
WEI Monitoring	Service that monitors all messages exchanged with the ERP.
WPA	Wi-Fi Protected Access; security protocol used in wireless networks

3 Introduction to the MES Infrastructure

This chapter describes the MES IT infrastructure supported by PAS-X.

3.1 Typical PAS-X MES Infrastructure



3.1.1 DMZ 3/4 (Interfacing Zone)

3.1.1.1 Interfacing Container Host

Hosts the interfaces for communication with another level.

Only required for integration with other levels and therefore optional.

3.1.1.2 Client Virtualization

The Client Virtualization is a technology that separates the desktop environment (including the application software) from the physical device used to access the application software.

For PAS-X, the Client Virtualization can be used to provide access to the PAS-X Client software.

It is possible to set up a PAS-X System without using Client Virtualization.

3.1.2 Level 3 (Manufacturing Operations Management)

3.1.2.1 Management Host

It is used for executing the deployment of PAS-X to the Clustered Container Hosts.

The deployment process itself will be run inside a Docker Container therefore the Management Host needs to be based on Linux and Docker.

3.1.2.2 PAS-X Core Components

Core components are essential for any MES. An MES mainly consists of the following core components:

3.1.2.2.1 PAS-X Clustered Container Hosts

The PAS-X Clustered Container Hosts hold all PAS-X core components (also known as services):

- Reverse proxies (for encrypted communication – will be delivered with PAS-X)
- RabbitMQ (will be delivered with PAS-X)
- Exceptions: integration with automation (Level 2) and client

The cluster is built by using an orchestrator (Docker Swarm or Kubernetes).

3.1.2.2.2 Database

The database is the repository for the business data processed by PAS-X. For further details see section: [Database](#).

3.1.2.3 Client Virtualization

The Client Virtualization is a technology that separates the desktop environment (including the application software) from the physical device used to access the application software.

For PAS-X, the Client Virtualization can be used to provide access to the PAS-X Client software.

It is possible to set up a PAS-X System without using Client Virtualization.

3.1.2.4 DMZ 3/3 (Interfacing Zone)

3.1.2.4.1 Interfacing Container Host

Hosts the interfaces for communication with another level.

Only required for integration with other levels and therefore optional.

3.1.3 DMZ 2/3 (Interfacing Zone)

3.1.3.1 Interfacing Container Host

Hosts the interfaces for communication with another level.

Only required for integration with other levels and therefore optional.

3.1.3.2 Interfacing Windows Host

Hosts the Windows-specific interfacing software for communication with another level.

Only required for integration with other levels and therefore optional.

3.1.3.3 Client Virtualization

The Client Virtualization is a technology that separates the desktop environment (including the application software) from the physical device used to access the application software.

For PAS-X, the Client Virtualization can be used to provide access to the PAS-X Client software.

It is possible to set up a PAS-X System without using Client Virtualization.

3.1.4 Corporate Level

3.1.4.1 LDAP

LDAP or Active Directory is used for user authentication while rights and role management are applied in PAS-X internally.

3.1.4.2 File Service (NFS)

PAS-X uses an SMB compatible file system to store and exchange documents.

3.1.4.3 Mail Service

PAS-X uses an SMTP compatible e-mail server to send out messages.

3.1.4.4 NTP

i All hosts shall be time synchronized using an NTP server.

3.1.4.5 CUPS Server(s)

CUPS is a modular print management system for Unix-like computer operating systems and is based on a client-server architecture.

Printing in PAS-X follows a modular approach, which allows running the system with multiple instances of the PAS-X Printing Service and multiple instances of the CUPS Server. As the CUPS Server implements communication via HTTP/IPP, it is possible to run the CUPS Server instances at different locations and zones of the network.

Each PAS-X Printing Service must be assigned to communicate to one of the available CUPS Servers. CUPS acts as an interface to printers and therefore has to communicate with them.

3.1.5 PAS-X Client Options

The PAS-X client enables the user to interact with PAS-X. It can be:

- Made available by using client virtualization technologies (such as Citrix)
- Operated on fat client machines.

PAS-X clients can be operated through all levels. For detailed information see section: [PAS-X Client](#).

3.2 PAS-X Optional Components

The following chapters describe components which are needed only for some special MES environments.

3.2.1 PDF/A conversion

PDF/A is an ISO-standardized version of the Portable Document Format (PDF) designed for the digital preservation of electronic documents. It will be used for long-term archiving of PAS-X BRR or label print by the PAS-X Central Service. The PDF/A conversion will be done by Ghostscript.

i Ghostscript is to be provided by the customer and will be deployed together with PAS-X Central Service automatically.

3.2.2 PAS-X Monitoring Service

PAS-X Monitoring Service is a long-term monitoring service for PAS-X service components.

3.2.3 PAS-X Authentication Adapter

The Authentication Adapter (AUDA) connects to external systems, which implement the External authentication interface, e.g. for authentication via card readers. It communicates via HTTP(S) with the external systems. If external authentication is not used, this service is not needed.

3.2.4 Deployment registry

If there is no local registry available as part of the infrastructure, the deployment registry can optionally be deployed with the System Manager.

It is a docker registry to store and provide images for the PAS-X deployment. It is used for the following objects:

- The delivered container images
- The images created at deployment time

4 Requirements

4.1 Container Orchestration Platform

PAS-X Server side components can be deployed and operated by using one of the following supported *Container Orchestration* platforms:

- Docker Swarm
- Kubernetes

i Only one of the above mentioned Container Orchestration platforms can be used for operating PAS-X at a time.

Detailed version information for each mentioned software can be found in the section [PAS-X runtime configuration](#).

i PAS-X will be delivered and operated by using Linux Containers.

4.1.1 Docker Swarm

4.1.1.1 Docker Swarm General

Docker Swarm is a container orchestrator and is a feature set of the Docker software itself.

A Docker Swarm is a group of either physical or virtual machines that are running the Docker application and have been configured to join together in a cluster. In context of PAS-X, it is used to ensure the following operational aspects:

- Multi-host networking
- Load balancing
- (High) availability

i In context of PAS-X, Docker Swarm is operated on Linux (see [PAS-X System Services](#) for details).

4.1.1.1.1 Docker Swarm High Availability Support

Docker Swarm is used to ensure the availability of all hosted PAS-X services.

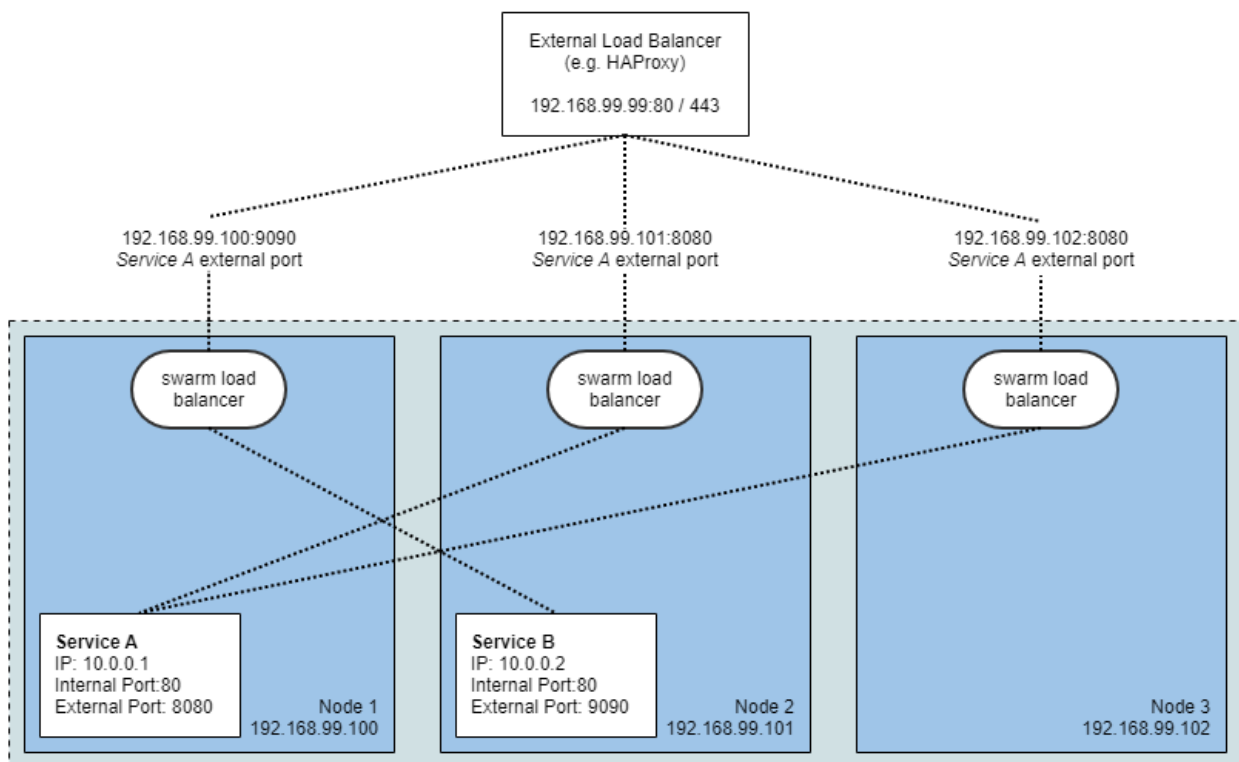
It is possible to size the infrastructure in a way that allows for rescheduling of PAS-X services in case of the loss of one (or more) Docker Swarm nodes.

i Keep in mind that starting a certain service might need some startup time. In conclusion: even if the system state is guaranteed, a service might be unavailable due to startup times.

i For information about the availability of Docker Swarm itself, please refer to [Docker Swarm Configuration](#).

In order to support better availability of PAS-X, it might be desired to run an external load balancer in front of the Docker Swarm. By doing so, the failure of a Docker Swarm Manager node will not lead to the unavailability of PAS-X. All network communication will be rerouted to another Docker Swarm Manager (restrictions are described in [Host bound PAS-X Services](#)). In addition, the Docker Swarm can be addressed via one IP address / hostname.

The following drawing shows this on a conceptual level:



i External load balancing capabilities, other than those by Docker Swarm itself, are not provided by Körber Pharma Software.

i Running an external load balancer might require to apply additional (high) availability concepts to such a load balancer.

i PAS-X does currently not support *dnsrr mode* (which is described in the Docker documentation).

For more detailed information please refer to <https://docs.docker.com/engine/swarm/ingress/>.

4.1.1.1.2 Docker Swarm Multi-Host Networking

Docker Swarm is used to build virtual multi-host networks (referred to as overlay networks).

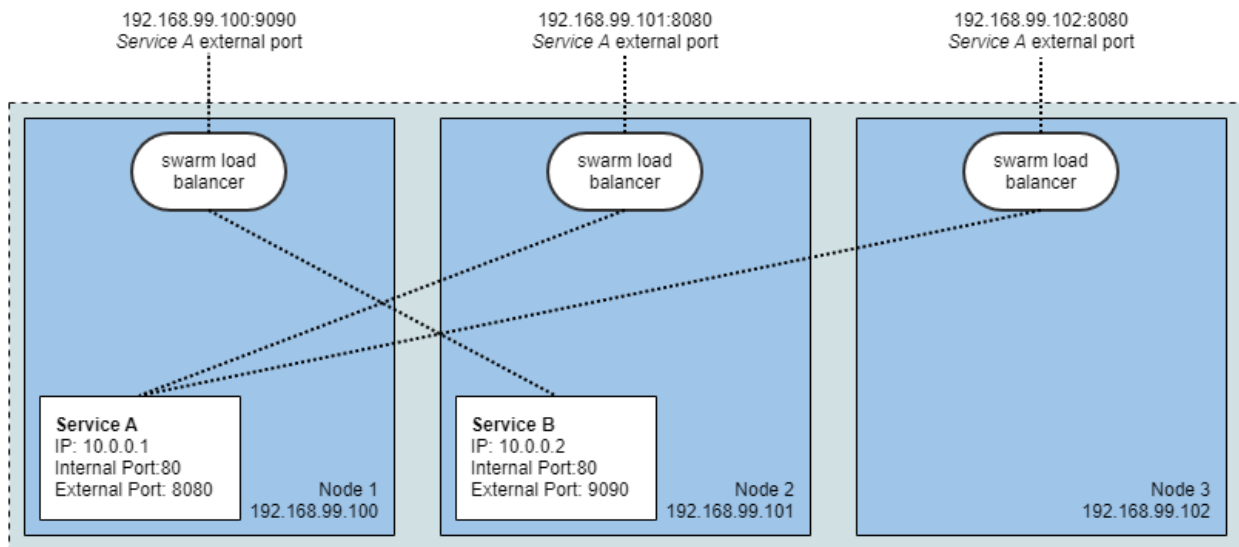
The PAS-X deployment creates such a network automatically on an existing Docker Swarm. In addition, it is ensured that all communication via the multi-host network is encrypted.

For more information, see the official Docker Documentation: <https://docs.docker.com/network/overlay/>

4.1.1.1.3 Docker Swarm Routing Mesh

Docker Swarm is used to dynamically distribute the PAS-X services on the different Swarm Worker Nodes. It is not required to address a specific Swarm node in order to communicate with a certain PAS-X service. Each Docker Swarm manager node holds the state of the cluster and is able to route the network traffic to a requested PAS-X service.

The following drawing shows different scenarios:



Most PAS-X services are operated as single instance services.

4.1.1.2 Docker Swarm Requirements

Requirements to deploy and operate PAS-X on Docker Swarm:

- Any Linux (x86_64 / amd64) distribution supported by Docker CE (for details, see <https://docs.docker.com/engine/install/>)
- A server running [Common Unix Printing System \(CUPS\)](#).
- PAS-X will be deployed by using a dedicated management node based on Linux.
- A set of Linux based machines acting as a cluster (Docker Swarm).

4.1.1.3 Docker Swarm Configuration

4.1.1.3.1 Cluster Sizing

A minimal Docker Swarm Setup consists of at least three compute nodes, all of them configured as *Swarm Manager*.

i One compute node can act as *Worker Node* **and** *Swarm Manager*. This is the default configuration when promoting a node to become a Swarm Manager.

i Körber Pharma Software recommends a setup with at least three compute nodes, each of them configured to act as Swarm Manager **and** Worker Node.
For an individual system sizing, please get in contact with Körber Pharma Software.

The following information refers to a different source from which the text was quoted. See: Official Docker Documentation. URL: <https://docs.docker.com/ee/ucp/admin/configure/join-nodes/>, retrieved 26 Feb 2020.

Docker Universal Control Plane is designed for High Availability (HA). You can join multiple manager nodes to the cluster. Thus, if one manager node fails, another can automatically take its place without impact to the cluster.

Having multiple manager nodes in your cluster allows you to:

- Handle manager node failures
- Load-balance user requests across all manager nodes.

Size your deployment

To make the cluster tolerant to more failures, add additional replica nodes to your cluster.

Manager nodes	Failures tolerated
1	0
3	1
5	2

For production-grade deployments, follow these rules of thumb:

- For high availability with minimal network overhead, the recommended number of manager nodes is 3. The recommended maximum number of manager nodes is 5. Adding too many manager nodes to the cluster can lead to performance degradation, because changes to configurations must be replicated across all manager nodes.
- When a manager node fails, the number of failures tolerated by your cluster decreases. Don't leave that node offline for too long.
- You should distribute your manager nodes across different availability zones. This way your cluster can continue working even if an entire availability zone goes down.

4.1.1.3.2 Network Configuration

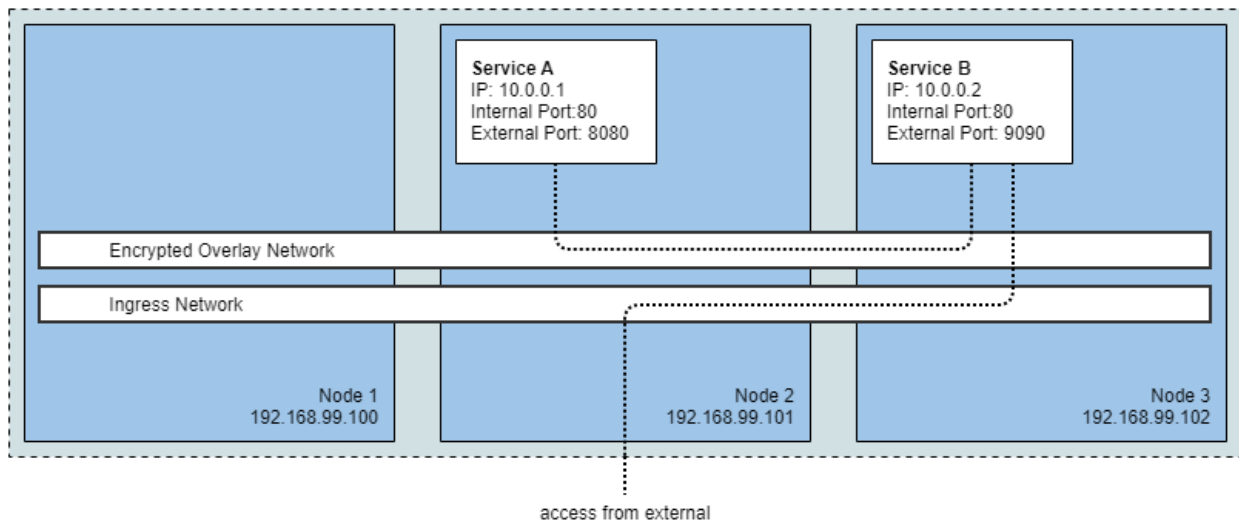
4.1.1.3.2.1 Overlay Networks

One of the key features of Docker (Swarm) are the networking capabilities.

For the deployment of PAS-X the capability to create overlay networks is essential. For usage of an overlay network, Docker creates a distributed network among multiple Docker daemon hosts. Such a network sits on top of (overlays) the host-specific networks, allowing containers connected to it (including swarm service containers) to communicate securely when encryption is enabled. Docker transparently handles routing of each packet to and from the correct Docker daemon host and the correct destination container.

Services that should be accessed from outside the Docker Swarm are part of a second network - the *ingress network*. The ingress network is a special version of an overlay network.

When deploying PAS-X IPSEC encrypted overlay networks are created automatically (see <https://docs.docker.com/network/overlay/> for more details on this topic).



4.1.1.3.2.2 Docker Default IP Addresses

The default address pools of docker are as follows:

Type	Default Size	Default Pool
global	/24	10.0.0.0/8
local	/16	172.17.0.0/12
local*	/20	192.168.0.0/16

* Local networks are allocated from 172.17.0.0/12, and then 192.168.0.0/16 once 172.17.0.0/12 is exhausted.

By default, Docker Swarm uses a default address pool 10.0.0.0/8 for global scope (overlay) networks. Every network that does not have a subnet specified will have a subnet sequentially allocated from this pool (*Default Size*). In some circumstances it may be desirable to use a different default IP address pool for networks. If the default 10.0.0.0/8 range conflicts with already allocated address space in your network, Körber Pharma Software strongly recommends ensuring that IP address ranges / pools for Docker managed networks are specified explicitly.

i It is mandatory to reserve IP address ranges for the usage by Docker / PAS-X.

During the Deployment of PAS-X, several networks are created which requires a certain Docker daemon and Docker Swarm configuration.

4.1.1.3.2.3 IP Address Ranges and Docker Configuration

For deploying PAS-X **two** class C IP network ranges are required.

- one address pool for the Docker Daemon (local scoped networks) - CIDR /26
- one address pool for the Docker Swarm (global scoped networks) - CIDR /24

On all Hosts running Docker create the following file in order to explicitly configure the IP addresses to be used:

/etc/docker/daemon.json

```
{
  "default-address-pools": [{"base": "x.x.x.x/26", "size": 29}]
}
```

When initializing the Swarm run the following command in order to explicitly configure the IP addresses to be used:

Swarm Initialization

```
docker swarm init --default-addr-pool y.y.y.y/24 --default-addr-pool-mask-length 26
--advertise-addr <local-ip-address>
```

i x.x.x.x and y.y.y.y are address pools.

i The *daemon.json* file and the *docker swarm init* command can be extended to system-specific needs.

4.1.1.3.3 Docker Remote API Access

4.1.1.3.3.1 With activated deployment option 'plain-socket-connection'

For Docker remote API access, port 2375 needs to be opened for the Docker daemon.

/etc/systemd/system/docker.service.d/options.conf

```
[Service]
ExecStart=/usr/bin/dockerd -H unix:// -H tcp://0.0.0.0:2375
```

Once this is done, execute

```
$ systemctl daemon-reload
$ systemctl restart docker
```

i The Docker remote API currently allows unauthenticated access.
It is strongly recommended to block connections to this network port from outside the PAS-X Docker environment.

4.1.1.3.3.2 With activated deployment option 'ssh-socket-connection'

Open port 2375 is not used any more for communication.

```
/etc/systemd/system/docker.service.d/options.conf
```

```
[Service]
ExecStart=/usr/bin/dockerd
```

Instead a ssh user with ssh-key needs to be prepared and configured at least for the core-services deployment-unit. This user is required at least on the first manager node and requires access to the Docker daemon.

4.1.1.3.4 RabbitMQ node labels

To prepare the Docker Swarm for the RabbitMQ HA deployment not bound to manager nodes (option `rabbitmq-ha-labeled`), the target nodes need to be labeled with `rabbitmq-node: yes`.

This has to be done for an odd number of nodes because RabbitMQ needs an odd number of instances to form a working cluster.

```
docker node update --label-add rabbitmq-node=yes <node-id>
```

4.1.1.4 Encrypted Communication with PAS-X

When using encrypted communication, the reverse proxy traefik handles all encrypted traffic. Therefore, a certificate in .pem format needs to be available for the traefik (which will be deployed with PAS-X).

- It is a format encoded in Base64 with ASCII characters.
- The extensions .cer, .crt, .pem or .key (for the private key) are most often used for these certificates.
- Apache and servers on Unix / Linux OS assume this format.

4.1.1.5 Docker Swarm Restrictions

4.1.1.5.1 Antivirus Software

When antivirus software scans files used by Docker, they may be locked in a way that causes Docker to hang.

Add the Docker data directory to the exclusion list of your antivirus software to address this problem.

 The Docker data directory is `/var/lib/docker`

See <https://docs.docker.com/engine/security/antivirus/> for more details on this topic.

4.1.1.5.2 Host bound PAS-X Services

Even though, one of the main concepts of Docker Swarm is that services are not bound to a certain host, PAS-X requires to bind certain services to specific hosts (e.g. RabbitMQ Service in single instance deployment).

If e.g. the RabbitMQ host fails to operate, PAS-X will become unoperable.

For RabbitMQ, there are also options for a HA deployment (see section: RabbitMQ HA deployment options). Otherwise, to overcome this and in order to ensure system availability, Körber Pharma Software recommends to use availability features on hypervisor level (such as VMWare HA).

4.1.1.5.3 Intrusion Detection/Prevention Systems

The following software categories may cause an impact to the operation of the PAS-X system or the PAS-X runtime stack.

- Intrusion Detection Systems (network and host-based)
- Intrusion Prevention Systems (network and host-based)
- Deep Packet Inspection firewalls
- Configuration Management tools (e.g. Puppet, Chef)
- Antivirus Software

This is due to the fact that these types of software dynamically adapt system behavior or influence network communication.

4.1.1.5.3.1 Local Firewall

Docker heavily relies on the Linux feature *iptables*.

Running a local *iptables* based firewall (e.g. *firewalld*) on a Docker host might interfere with Docker itself. Ensure a specific starting order on all involved hosts: local firewall first, docker second.

i If you are running tools that ensure a specific host state by regularly running tasks (e.g. puppet), make sure that you do **NOT** change *iptables*/firewall rules during operation of Docker.

i Always stop docker itself before applying new firewall rules.

i Werum strongly recommends **not** to use *firewalld* in combination with Docker.

4.1.1.5.4 SELinux

Security-Enhanced Linux (SELinux) is a security architecture for Linux operating systems that allows more fine-grained access control.

When enabled, SELinux can be configured in two modes:

- *Enforcing*: SELinux policy is enforced and access is denied based on defined policy rules.
- *Permissive*: SELinux policy is not enforced and only logs actions that would have been denied in enforcing mode.

Docker allows to enable SELinux in the docker daemon configuration file (*/etc/docker/daemon.json*).

⚠ PAS-X does not support SELinux in *enforcing* mode when SELinux is also enabled in the docker daemon configuration!

4.1.1.6 PAS-X and Docker Enterprise Features

i PAS-X is released for use with Docker Community Edition (CE).
For running PAS-X on Docker Enterprise Edition (EE) please make sure that a corresponding platform release is available.

In addition, the restrictions/additions in the sections below apply.

4.1.1.6.1 Additional Resources (RAM, CPU)

When dimensioning the hosts for running PAS-X, it must be taken into account that Docker EE features are running as a set of Docker containers which have their own resource footprint (RAM, CPU).

The required resources have to be added to those resources required for running PAS-X.

4.1.1.6.2 Universal Control Plane

The PAS-X deployment process relies on communication with Docker via network port 2375. This is discouraged by some Docker EE features.

If Docker EE features, e.g Universal Control Plane (UCP), are to be deployed, it is required to provide an additional parameter in order to allow for communication via network port 2375:

```
--force-insecure-tcp
```

4.1.1.7 NFS

The Network File System (NFS) is a distributed file system protocol that allows shared file access over the network.

i In a PAS-X environment, an NFS server is required to persist certain information (e.g. log files and documents) and make it available outside the container environment.

The directory structure for the NFS has to be created with the service users in mind. See also section: [Service users](#). The directories for the services have to allow access for the users of the services.

4.1.1.7.1 Export service directories for log and external document files

4.1.1.7.1.1 Providing the directory structure

1. Create export root- and sub-directories, see below for which directories are necessary

```
sudo mkdir -p <export-root-directory> # e.g. for a PAS-X system named "pasx":
sudo mkdir -p /mnt/pasx
# for all services
sudo mkdir -p <export-sub-directory> # e.g. for PAS-X service "central": sudo
mkdir -p /mnt/pasx/central
sudo chown <service-user> <export-sub-directory> # e.g. for PAS-X service
"central" and user "pasxuser": sudo chown pasxuser /mnt/pasx/central
# Optionally for CUPS:
sudo mkdir -p <export-sub-directory_cups> # e.g. for CUPS: sudo mkdir -p /mnt/
pasx/cups-pdf
```

2. Export the desired export directories by adding them subsequently to file "/etc/exports" for all hosts of the PAS-X Swarm:

```
echo "<export-root-directory>
<DOCKER_SWARM_NODE1>(rw,fsid=0,insecure,no_subtree_check,async,no_auth_nlm,no_roo
t_squash)
<DOCKER_SWARM_NODE2>(rw,fsid=0,insecure,no_subtree_check,async,no_auth_nlm,no_roo
t_squash)" > /etc/exports
# for all <export-sub-directory>s
echo "<export-sub-directory>
<DOCKER_SWARM_NODE1>(rw,nohide,insecure,no_subtree_check,async,no_auth_nlm,no_roo
t_squash)
<DOCKER_SWARM_NODE2>(rw,nohide,insecure,no_subtree_check,async,no_auth_nlm,no_roo
t_squash)" >> /etc/exports
#...
# Optionally for CUPS:
echo "<export-sub-directory_cups>
<CUPS_HOST>(rw,nohide,insecure,no_subtree_check,async,no_auth_nlm,no_root_squash)
" >> /etc/exports
```

3. Afterwards, set the new exports effective via following command:

```
/usr/sbin/exportfs -rv
```

4.1.1.7.1.2 Necessary directories

Which directories are necessary depends on the *services* and *options* selected in the deployment configuration.

The `export-root-directory` can be chosen freely. The names of the sub-directories have to match the expected names because they are exported with and addressed by their actual names.

Service	Option	Directories to create
all	log-shared-folder	<p>A directory for each service in the platform specification's <code>services</code> block (<code>platform-specification.deployment.services</code>) where the directory name is exactly the same as the service name in the <code>services</code> block.</p> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>platform-specification</p> <pre>platform-specification: deployment: services: - auda - central - configservice ... options: - log-shared-folder ...</pre> </div> <p>These directories have to be created:</p> <ul style="list-style-type: none"> • <code><export-root-directory>/auda</code> • <code><export-root-directory>/central</code> • <code><export-root-directory>/configservice</code> • ...
central	central-shared	<p>These directories have to be created:</p> <ul style="list-style-type: none"> • <code><export-root-directory>/central-shared/LabelLogArchive</code> • <code><export-root-directory>/central-shared/pasx_archive</code> • <code><export-root-directory>/central-shared/pasx_archive_mbr</code> • <code><export-root-directory>/central-shared/SavedDocuments</code> • <code><export-root-directory>/central-shared/ExternalDocuments</code> • <code><export-root-directory>/central-shared/AsyncDocuments</code> • <code><export-root-directory>/central-shared/AsyncDocumentsErrors</code>

Service	Option	Directories to create
cups	-	These directories have to be created: <ul style="list-style-type: none"> • <code><export-root-directory>/cups-pdf</code>
all	languagepack	These directories have to be created: <ul style="list-style-type: none"> • <code><export-root-directory>/languagepack</code>
<ul style="list-style-type: none"> • label-printing • report-printing 	reports-shared-folder	These directories have to be created: <ul style="list-style-type: none"> • <code><export-root-directory>/custom-reports</code>
pasx-monitoring	pasx-monitoring-shared-folder	These directories have to be created: <ul style="list-style-type: none"> • <code><export-root-directory>/pasx-monitoring</code>

4.1.1.7.2 NFS Security

The exported NFS shares need to be available to the following network resources:

- Docker Swarm Nodes (for persistence of technical logfiles)

Access to the NFS volumes can be limited within the NFS exports configuration (*/etc/exports*) or by dedicated firewall rules.

4.1.1.8 Service users

PAS-X System services are running with a user (and optionally a group) configured for the deployment. This allows the services to run with a non-root user.

In a production deployment, the following has to be considered:

- In general, the user ID and group ID used for the services do not have to exist on the host machines. Exceptions to this rule are described below.
- The Service Router (Traefik) needs access to the Docker daemon socket of the host.
 - By using the option `plain-socket-connection`, Traefik service has to run as a user or group which exists on that host and has Docker access rights assigned. This is by default not the case. The Service Router is deployed to one of the manager nodes of the Swarm. This means that the user or group used for the Service Router has to be an existing user or group on the manager nodes of the Swarm with Docker access rights.
 - Since 3.3.2 using the deployment option `ssh-socket-connection` is recommended. This implies no placement constraint anymore and using user `nobody` for execution of the Service Router.
- In a default deployment, the services read from and write to a shared file system provided by the NFS. Therefore, the user or group used for the services has to exist on the NFS host and needs write access to the directories shared on the NFS.

- PAS-X Monitoring Service has to run as root.
- The Deployment Registry has to run as root.

In non-production deployments, external services like NFS or CUPS are also provided with the PAS-X deployment. Those services may run as root.

4.1.2 Kubernetes

4.1.2.1 Kubernetes General

Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.

4.1.2.2 Kubernetes Requirements

PAS-X is released for use with a specific Kubernetes API version. See [Server](#) for further information on the API version.

PAS-X deployment is done based on Helm. See [Server](#) for further information on the used Helm version.

The Kubernetes cluster has to provide sufficient resources for running PAS-X workloads. See [Systems Sizing Introduction](#) for further details on Systems Sizing.

4.1.2.3 DNS

PAS-X MES deployment comes with a set of ingress objects. The PAS-X instance running in the Kubernetes cluster is resolved via a subdomain. The corresponding sub domain needs to be available in the DNS.

4.1.2.4 Windows Fileshares with Kubernetes

When operating PAS-X it might be required to provide user access to PAS-X generated content (e.g. PDFs). In addition it might be desired to let system users add/change print templates (Crystal Reports templates). Therefore the following services request PVC - Persistent Volume Claims:

Service	PVC Name	Access Mode
Central	pvc-central-shared-files	ReadWriteMany
PASX-Monitoring	pvc-pasx-monitoring-database	ReadWriteMany
Label-Printing	pvc-label-printing-custom-reports	ReadOnlyMany
Report-Printing	pvc-report-printing-custom-reports	ReadOnlyMany

4.1.2.4.1 Requirements

For each persistent claim, a PVC with the name specified above must be created in the namespace where PAS-X is installed.

PVC Central Example

```
#
# Example to create the persitent volume claim for the central service.
#
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  #
  # PVC Name used by the central service
  #
  name: pvc-central-shared-files
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      #
      # Adjustment of the size to the desired requirements
      #
      storage: 100Gi
  #
  # Usage example of a dedicated cluster volumen
  #
  volumeName: pv-central-shared-files
  #
  # Alternative use a storage class to provide persistence
  #
  storageClassName: "<storage-class-to-be-used>"
```

4.1.2.4.2 Windows SMB Server example

In case that a Windows integration (smb protocol) for above mentioned use cases is desired, it is possible to use the *SMB CSI Driver for Kubernetes*.

Other technical solutions are also possible and can be setup as needed. Please refer to <https://kubernetes.io/docs/concepts/storage/persistent-volumes/#types-of-persistent-volumes> for further information on Kubernetes supported plugins.

4.1.2.4.2.1 Secrete

The following example is based on a sceret that provides the necessary access parameters for a Windows SMB export.

Example Secrete

```
#
# Creates a used in the example below
#
kubectl create secret generic smbcreds \
  --from-literal username=<username> \
  --from-literal password="<userpassword>" \
  --from-literal domain="<userdomain>"
```


If no domain is required for the desired user, it can be omitted.

4.1.2.4.2.2 SMB CSI Driver for Kubernetes

SMB CSI Driver Example

```
#
# Creates a persistent volume to provide this storage to a persistent volume claim
#
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: smb-example-storage-class
provisioner: smb.csi.k8s.io
parameters:
  source: "//server-to-be-used/export-folder"
  subDir: "sub-dir-for-example-the-service-name"
  csi.storage.k8s.io/provisioner-secret-name: "smbcreds"
  csi.storage.k8s.io/provisioner-secret-namespace: "default"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
volumeBindingMode: Immediate
mountOptions:
  - dir_mode=0777
  - file_mode=0777
  - uid=1001
  - gid=1001
  - noperm
  - mfsymlinks
  - cache=strict
  - noserverino # required to prevent data corruption
```

4.1.2.4.3 References

- Kubernetes.io : <https://kubernetes.io/docs/concepts/storage/persistent-volumes/>

4.1.2.5 Observability

All microservices implement Spring Actuator HTTP endpoints for observability. The endpoints can be reached cluster-internally on each pod.

- Port : 8087
- Path: `/monitoring/`

The page is a guide to further metrics implemented by the service.

i Some metrics are only reachable by specifying the credentials set on deployment.

4.1.2.5.1 Prometheus Monitoring

All services support Prometheus monitoring. Therefore, the pods are annotated with the attributes `path`, `port` and `scrape`.

Prometheus

```
prometheus.io/path=/monitoring/prometheus
prometheus.io/port=8087
prometheus.io/scrape=true
```

Most services follow the default attributes. In case of non-default values, the annotation documents the current set value.

4.1.2.5.2 References

- [Spring Boot - Actuator](#)
- [Spring Boot - Actuator Metrics](#)

4.1.2.6 Expose RabbitMQ for access from outside Kubernetes

PAS-X MES uses RabbitMQ as a message broker.

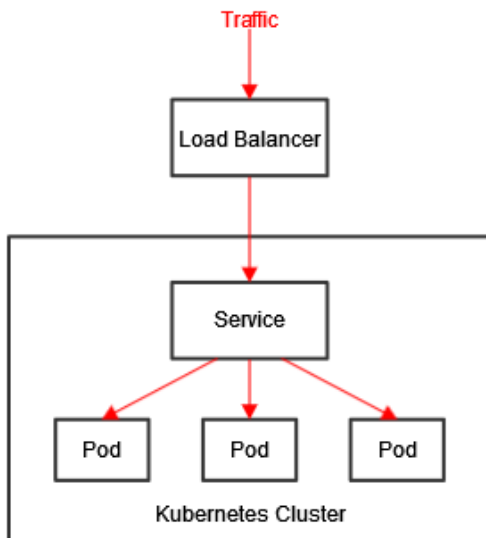
For some use cases it is required to access RabbitMQ from outside the Kubernetes cluster (e.g. Level 2 integration (DCS)).

How to expose RabbitMQ to the outside depends on the specific environment (Kubernetes cluster setup/ configuration/ public cloud / on- vs off-premise). The three options for exposing RabbitMQ are described as follows.

i Some system specifics are heavily depending on the individual infrastructure and therefore there is no general solution available.

4.1.2.6.1 Automatic Load Balancer Configuration

If the cluster provider supports this option, it is possible to use a *LoadBalancer* Service to automatically configure (and reconfigure) the external load balancer, that will forward the traffic to the nodes of a cluster. This scenario is typically desirable for systems running in the public cloud.



Further details are available via the [official Kubernetes documentation](#).

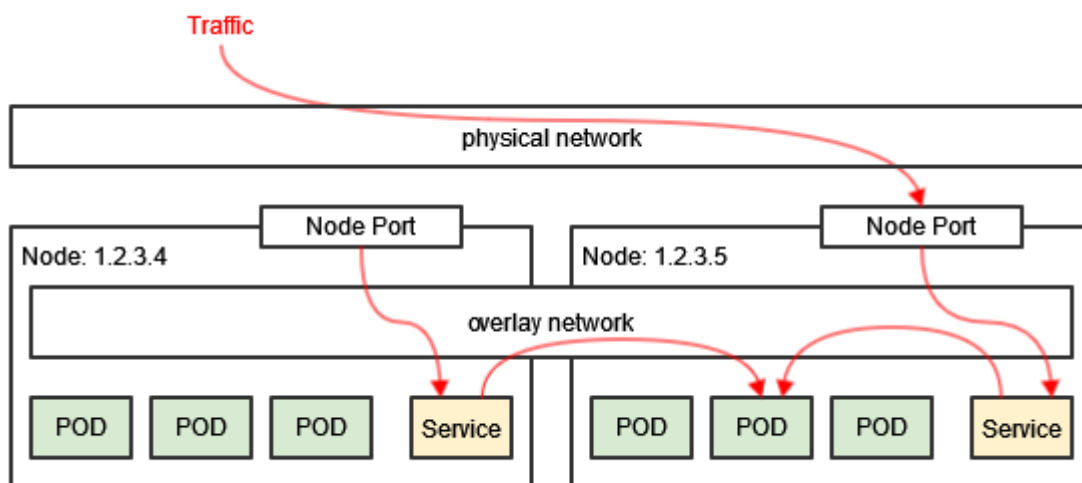
[Microsoft Azure](#) and [AWS](#) provide further information on this topic. Other cloud providers might have comparable solutions available.

i *Automatic Load Balancer Configuration* is recommended for productive use but is only available if the cluster provider supports this option.

4.1.2.6.2 Node Port

A Node Port Service will open a port on all nodes of the cluster, to make the pods available. The port number can be automatically chosen by Kubernetes, or manually specified. But it must lie in the range 30000-32767 (by default).

This concept will work on any Kubernetes cluster.



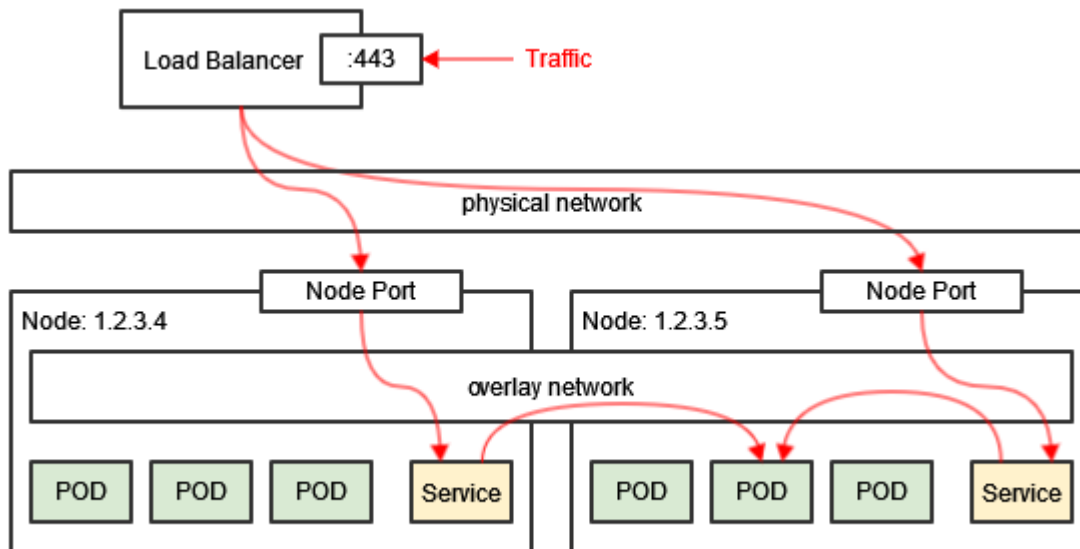
i Network communication will typically be done via a specific node/host IP.

i The Node Port concept should not be considered for productive scenarios as this concept relies on the availability of a certain node, thus no high availability can be guaranteed.

Further details are available via the [official Kubernetes documentation](#).

4.1.2.6.3 Node Port and Manual Load Balancer Configuration

A first solution consists in using a Node Port Service to expose the app on all nodes, on a fixed port (for example 30155). Then an external level 4 load balancer can be used to forward the traffic to the nodes of the cluster. Usually these type of load balancers are able to detect unreachable nodes, so traffic will automatically be forwarded to available nodes in the cluster, to provide high availability.

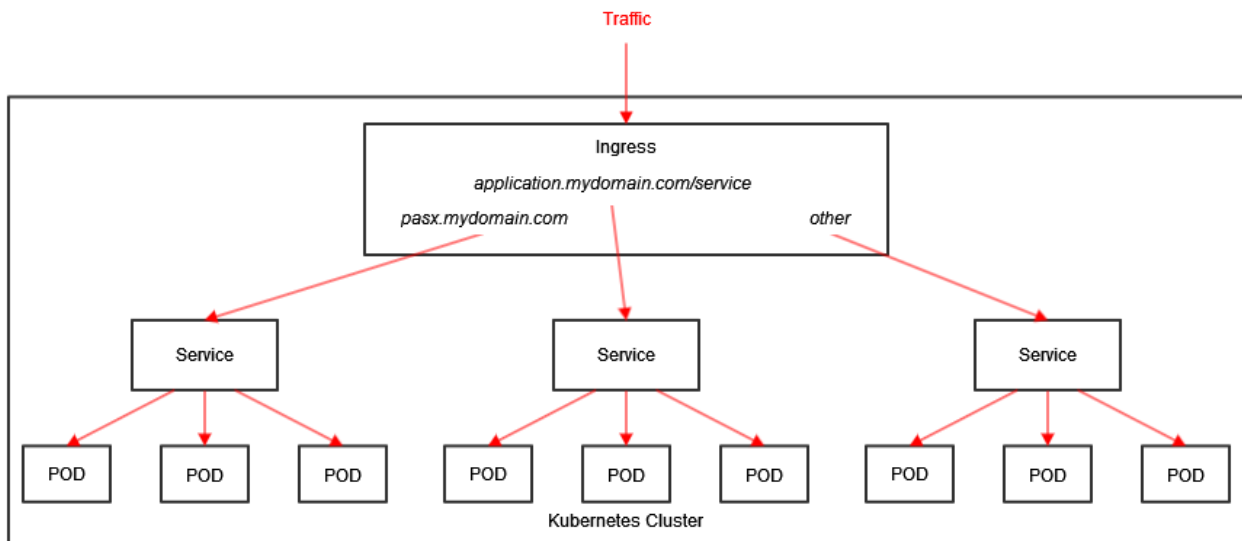


i Node Port and Manual Load Balancer Configuration can be used for productive scenarios.

i It is recommended to setup the external load balancer in a high available manner.

4.1.2.6.4 TCP Port Forwarding

Kubernetes uses the ingress concept which normally works on http/https. In a Kubernetes cluster, Ingress support can be established by using various [ingress controllers](#). Some available ingress controllers are able to provide load balancing capabilities (even on Level 4) which enables for TCP Port Forwarding.



Further information is available via the official Kubernetes documentation <https://kubernetes.io/docs/concepts/services-networking/ingress/>

i Not all available ingress controllers allow for TCP port forwarding and therefore TCP Port Forwarding via ingress might not be available in every Kubernetes Setup.

i It needs to be considered if the ingress controller can be operated in a high available manner for productive scenarios.

4.1.2.7 Multiple PAS-X MES Instances on one Kubernetes Cluster

It is possible to deploy more than PAS-X MES instance into one Kubernetes cluster.

- In general, it is required to have a dedicated Kubernetes namespace for one PAS-X MES instance.
- A separate database schema/user per PAS-X MES instance is required.
- A separate RabbitMQ instance per PAS-X MES instance is required (normally this will be ensured by PAS-X MES deployment).
- The specific PAS-X MES instance running in the Kubernetes cluster is resolved via a subdomain.
- The Ingress Controller needs to support sub-domains.

i Wildcard DNS entry is recommended in order to operate multiple PAS-X MES instances in one Kubernetes cluster.

i When multiple PAS-X instances are operated in a Kubernetes cluster, sufficient resources (RAM/CPU/Storage) have to be supplied. Sharing resources between PAS-X MES instances is not possible.

4.1.2.8 Ingress Timeout Configuration

The Ingress Configuration needs to be adjusted in order to operate PAS-X MES on Kubernetes properly

The relevant configuration shown below is based on nginx as the ingress controller. This can be adopted to other ingress controllers, if needed.

Property Name	Value	Description
nginx.ingress.kubernetes.io/proxy-connect-timeout	75	Defines a timeout for establishing a connection with a proxied server. Default is 60 seconds. It should be noted that this timeout cannot usually exceed 75 seconds.
nginx.ingress.kubernetes.io/proxy-next-upstream-timeout	0	Limits the time during which a request can be passed to the next server. Default is 0, the 0 value turns off this limitation.
nginx.ingress.kubernetes.io/proxy-read-timeout	3060	Defines a timeout for reading a response from the proxied server. The timeout is set only between two successive read operations, not for the transmission of the whole response. If the proxied server does not transmit anything within this time, the connection is closed
nginx.ingress.kubernetes.io/proxy-send-timeout	3120	Sets a timeout for transmitting a request to the proxied server. The timeout is set only between two successive write operations, not for the transmission of the whole request. If the proxied server does not receive anything within this time, the connection is closed.

4.1.2.9 Ingress Controller with Session Stickiness Capabilities

The deployment of PAS-X on a Kubernetes Platform requires some components with specific capabilities.

As the Kubernetes platform is designed to support failover and high availability (HA) features, underlying components like the ingress controller should be capable of supporting session stickiness.

Session stickiness is required for some PAS-X services - mainly if HA capabilities should be reached - and therefore have to be supported by the ingress controller (e.g. Nginx). The ingress controller sets a service specific cookie in the end user's browser to route incoming traffic to one Kubernetes replica instance.

In case of replicated PAS-X services, this session stickiness must be supported by the ingress controller of choice if an external (different from Nginx) ingress controller is chosen in a customer's Kubernetes environment. Note: Internal ingress controller configurations regarding sticky sessions have to be overwritten or adapted in case of external ingress controller use.

4.1.3 PAS-X System Services

The following containers/services (Docker Swarm) or Pods (Kubernetes) can be created during deployment:

4.1.3.1 PAS-X Services

Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X Authentication Adapter Service	authenticationadapter	auda	auda-deployment	Provides functionalities related to external authentication. The Authentication Adapter is an interface to external systems so that they can provide information about which user is logged in to which terminal, about failed login attempts and signatures provided externally.
PAS-X Central Service	central	central	central-deployment central-job	Provides the main PAS-X functionalities. This includes: <ul style="list-style-type: none"> • User, rights, and session management • MBR design • Order planning • EBR/order execution • BRR review • Equipment management • Print data management • Various master data management (e.g. material)

Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X Cockpit Service	cockpit	cockpit	cockpit-deployment	Provides the functionality to integrate small widgets of other PAS-X services into one UI. Contrary to the UI Aggregator, which integrates whole pages of other PAS-X services into one UI.
PAS-X Configuration Service	configservice	configservice	configservice-deployment configservice-job	Provides the functionality to configure configuration properties of all PAS-X services at a central place.
PAS-X Event Data Warehouse Service	edw	edw	edw-deployment edw-job	Provides the functionality to publish dedicated production data, which are used by external consumers, via Kafka.
PAS-X Equipment Service	equipment	equipment	equipment-deployment equipment-job	Provides the functionality for managing equipment and equipment-related dialogs.
PAS-X Execution Service	execution	execution	execution-deployment execution-job	Provides the functionality for task-based execution of ESPs.
PAS-X Import Export Service	importexport	importexport	importexport-deployment	Provides the functionality to transfer master data from one PAS-X instance to another.



Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X Message Monitoring Service	messagemonitoring	memo	memo-deployment memo-job	Provides the basic communication functionality of PAS-X. The message monitoring service is responsible for monitoring / handling errors in the delivery of RabbitMQ messages within PAS-X. It also allows triggering a resend of successful messages (in case RabbitMQ and database state need to be synchronized).
PAS-X MSI Service	msi	msi	msi-deployment	Provides functionalities for the integration of external shop floor systems into PAS-X. This service provides a message-based standard interface for communication.

Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X Notification Service	notification-service	nose	nose-deployment	<p>Provides functionalities for the notification of users and user groups in case respective events are sent by other PAS-X services.</p> <p>Currently, the following PAS-X services are sending events which are picked up and processed by the notification service:</p> <ul style="list-style-type: none"> ▪ Exceptions <ul style="list-style-type: none"> ▪ For every exception created in PAS-X an event is sent to the notification service ▪ WEI monitoring service <ul style="list-style-type: none"> ▪ For every incoming ERP message, an event is sent to the notification service ▪ For every outgoing ERP message, an event is sent to the notification service
PAS-X Order Review service	orderreview	orderreview	orderreview-deployment	Provides the functionality to reviewing task-based order executions.
PAS-X Print Service	print	printing	label-printing-deployment report-printing-deployment	Provides functionalities related to PAS-X printing. The print service is responsible for creating labels or reports (as PDFs) and sending them to a printer. The technology used for creating the PDFs is Crystal Reports.



Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X Replenishment Service	replenishment	replenishment	replenishment-deployment	Provides replenishment functionalities. Replenishment is the process to refill the production facility with material. Based on a selection of orders and their required material demand, the replenishment will give the operator an overview of missing material in the production.
PAS-X Scale Service	scaleservice	scls	scls-deployment	Provides functionalities to connect scales for weighing operations in PAS-X. A PAS-X system may have more than one scale service instance and a scale service instance may have more than one connected scale.
PAS-X Storage Tracking Service	storagetracking	str	str-deployment str-job	Provides functionalities for storage tracking in PAS-X.
PAS-X Task Service	task	task	task-deployment task-job	Provides the task management functionality. Tasks represent activities sent from other PAS-X services which users have to carry out in the PAS-X Cockpit. Manual work steps are a special kind of task which can be created directly in this service.

Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X UI Aggregator Service	uiaggregator	uia	uia-deployment	Provides functionalities to harmonize the user interfaces (UI) of other PAS-X services in order to get an integrated application frontend. This service is for example responsible for providing the navigation bar and handling (showing / hiding) the open UIs of the different PAS-X services in the web application.
PAS-X WEI Service	wei	wei	wei-deployment	Provides functionalities for the communication between PAS-X and an ERP system. ERP systems are connected through an XML-based web service.
	weirfc	weirfc	weirfc-deployment	Provides functionalities for the communication between PAS-X and an ERP system. ERP systems are connected through an SAP-specific RFC interface.
PAS-X WEI Monitoring Service	weimonitoring	weimon	weimon-deployment	Provides functionalities for monitoring the communication between PAS-X and an ERP system. This service is responsible for logging messages sent to and received from an ERP system. It can also be used to trigger re-sending of erroneous messages.



Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
PAS-X WMS Service	wms	wms	wms-deployment	Provides the Warehouse Management System (WMS) functionality. This service manages the stock and the localization of objects (transportable units) like storage units, carrier, order handling units and equipment.

4.1.3.2 PAS-X Simulators

Long name	Service ID	Technical Container ID	Pod Name (Kubernetes)	Description
ERP Simulation	–	erpsimulator	erpsimulator-deployment	The ERP simulator can be used to send ERP messages to PAS-X.
Simulator for MSI Shop Floor	–	msisimulator	msisimulator-deployment	Simulates an external shop floor system, connected to PAS-X.
Simulator to trigger AUDA	–	audasim	audasim-deployment	The Authentication Adapter Simulator can be used to simulate an external system.

4.1.3.3 Supporting Services

Long name	Service ID (Docker Swarm)	Technical Container ID (Docker Swarm)	Pod Name (Kubernetes)	Description
Help Service	–	help	help-deployment	Delivers Online Help.
Message Broker	–	rabbitmq	rabbitmq-<number>	A message broker, used for communication between PAS-X services.
Proxy & Service Router	–	traefik	–	A reverse proxy, used for accessing the separate PAS-X services via encrypted communication.
PAS-X Monitoring	–	pasx-monitoring	pasx-monitoring-deployment	PAS-X Monitoring

4.2 Client Peripherals

4.2.1 Client Screen Size

Minimum requirement for a screen for a PAS-X client is Full HD (1920 x 1080 pixel).

4.2.2 Barcode Scanners

Long- or short-range USB barcode scanners may be used depending on the intended application. USB barcode scanners should allow a configuration of the character send rate.

Compatible hardware: Data Logic, Symbol, Intermec.


4.3 Common Unix Printing System (CUPS)

PAS-X utilizes CUPS for executing print jobs.

CUPS is a modular print management system for Unix-like computer operating systems and it is based on a client-server architecture.

In the PAS-X context, the PAS-X printing service is acting as CUPS client sending PDF-based print jobs to the CUPS server.

For printing with PAS-X, it is required to have (at least) one printer configured in CUPS.

 The PAS-X printing service uses the Java library cups4j to communicate with the CUPS instance, e.g. to create print jobs. The currently used version of the cups4j library does not support authentication or encryption of the CUPS communication.

4.3.1 Supported printers

PAS-X supports all printers that are supported by the used CUPS system.

CUPS supports a printer, if the printer supports either Postscript or a printer language that is supported by the installed CUPS filter of the used CUPS system.

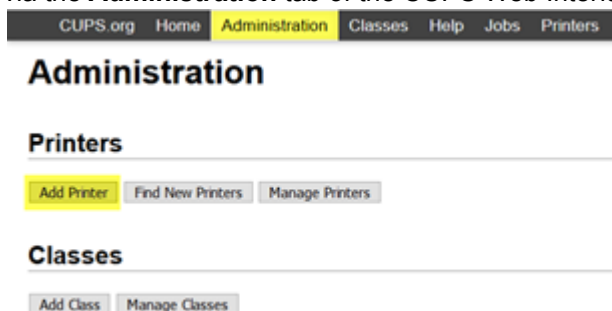
Based on the installed CUPS version the following approaches exist to clarify if the printer is supported:

CUPS version	Description
< 2.4.x	<p>Based on following statement the following CUPS filter are supported by default:</p> <p>The following information refers to a different source from which the text was quoted. See Wikipedia; URL: https://en.wikipedia.org/wiki/CUPS, retrieved 5 May 2021.</p> <ul style="list-style-type: none"> • raster to PCL • raster to ESC/P or ESC/P2 (an Epson printer language, now largely superseded by their new ESC/P-Raster format) • raster to Dymo (another printer company). • raster to Zebra Programming Language or ZPL (a Zebra Technologies printer language) <p>As of 2009 other proprietary languages like GDI or SPL (Samsung Printer Language) are supported by Splix, a raster to SPL translator. However, several other alternatives can integrate with CUPS. HPLIP (previously known as HP-IJS) provides Linux+CUPS drivers for HP printers, Gutenprint (previously known as Gimp-Print) is a range of high-quality printer drivers for (mostly) inkjet printers, and TurboPrint for Linux has another range of quality printer drivers for a wide range of printers.</p>
>= 2.4.x	<p>The OpenPrinting project provides the webpage https://www.openprinting.org/printers to easily check, if the printer is supported.</p>

4.3.2 Adding Printers to CUPS

To be available for PAS-X printing, printers must be added to CUPS. This can be done:

- by using the CUPS command-line printer administration interface (see <https://www.cups.org/doc/admin.html>)
– or –
- via the **Administration** tab of the CUPS Web Interface (**Add Printer** button)



! When adding a printer make sure to enable "sharing" for the specific printer. This can be done via UI and command line.

4.3.3 Configure PAS-X Printing Service to use CUPS

Printing in PAS-X follows a modular approach, which allows running the system with multiple instances of the PAS-X Printing Service and multiple instances of the CUPS Server.

As the CUPS Server implements communication via HTTP/IPP it is possible to run the CUPS Server instances at different locations and zones of the network.

Each PAS-X Printing Service must be assigned to communicate to one of the available CUPS Servers using the following service configuration properties:

Property	Description
printstrategy.cups.host	Defines the host name, e.g. <i>127.0.0.1</i> , on which the CUPS server runs.
printstrategy.cups.port	Defines the port, e.g. <i>631</i> , on which the CUPS server listens.

4.3.4 Configure PAS-X Printing Service

Further configuration of PAS-X printers and their assignment to specific report types can be done via the PAS-X function "Administration > Printers".

For further details see "PAS-X" reference manual; section "Printing".


4.3.5 CUPS Security

The CUPS web interface needs to be available for the following network resources:

- Docker swarm nodes (for the PAS-X printing service)
- CUPS administrators (e.g. for maintenance activities)

Access to the web interface can be limited within the CUPS configuration file (*/etc/cupsd/cupsd.conf*) or by dedicated firewall rules.

Currently, the PAS-X printing service does not support authentication and encryption when communicating with the CUPS service. However, it is strongly recommended to enable these security mechanisms for administrative functionality via the CUPS web interface.

 For details, please refer to the official CUPS documentation.

4.4 Database

One Relational Database Management System (RDBMS) is required, either Oracle or PostgreSQL. The database host must be reachable via ping from the management node where the System Manager will be executed.

For further details see sections below.

4.4.1 Oracle software requirements

4.4.1.1 Oracle version

See section: [PAS-X runtime configuration / Server](#).

! However, Operating Systems other than Microsoft Windows might generate additional effort and must be discussed individually with the Werum Project Team.

4.4.1.2 Oracle software components

PAS-X can be installed using either Oracle Standard or Oracle Enterprise Edition. All required Oracle software components will be included within the Oracle Standard Edition, which can be chosen as installation option during the software setup. For PAS-X, no other software components are required even if the installation is set up using Oracle Enterprise Edition.

4.4.2 Oracle database requirements

4.4.2.1 General

Oracle Database with an empty schema (schema name can be chosen individually), whose OS is on the **same timezone** as the PAS-X system.

From infrastructure perspective the Database needs to be located close to the PAS-X system (in regard to network latency).

4.4.2.2 Oracle database components

Only Oracle default components are required.

4.4.2.3 Oracle server mode

It is strongly recommended to run the database instance in Dedicated Server Mode.

4.4.2.4 Initialization parameters

The following tables describe the basic Oracle instance settings that are used to set up the system initially.

4.4.2.4.1 Initialization parameters

Parameter	Value
db_block_size	16384

Parameter	Value
open_cursors	600
job_queue_processes	12
deferred_segment_creation	FALSE
Processes	800 **
memory_target	2G **
memory_maxtarget	4G **
optimizer_secure_view_merging	FALSE
undo_retention	3600 **
nls_length_semantics	CHAR ***
open_links	8
audit_trail	NONE *

* If the internal Oracle auditing is needed and the audit_trail parameter is set to a value of "db", the **SYS.AUD\$** table should be regularly purged by the DBA.

** These parameters depend on the number of concurrent users in the MES system, the configuration of the PAS-X Wildfly Application Server and the details of the database server hardware. Furthermore, these values might need to be adjusted during the lifetime of the MES database. The values given above should be understood as minimum values only.

*** This parameter has to be BYTE during the DB creation and must be switched to CHAR after the creation process (as a post-DB creation task).

4.4.2.4.2 Database parameters

Parameter	Value
CHARACTER SET	AL32UTF8
NATIONAL CHARACTER SET	AL16UTF16

4.4.2.5 Encryption

To enable encryption of database traffic the SQLNET.ORA file and add the following values:

Variable name	Value
SQLNET.ENCRYPTION_SERVER	REQUIRED
SQLNET.ENCRYPTION_TYPES_SERVER	(AES256)

No special configuration of the client is needed.

4.4.2.6 User profile

A profile is a named set of resource limits and password parameters that restrict database usage and instance resources for a user. You can assign a profile to any user, and a default profile to all others. Each user can only have one profile, and creating a new one supersedes an earlier version.

You need to create and manage user profiles only if resource limits are a requirement of your database security policy.

Without any change, all required database users reside in the "default" user profile. To avoid password degradation for the required users, we strongly recommend setting the database parameter *PASSWORD_LIFE_TIME* to unlimited.

(SQL command: *ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME UNLIMITED*)

4.4.2.7 Tablespaces

The following table describes the required PAS-X Oracle tablespaces with their recommended initial sizes. The standard *SYSTEM* and *SYSAUX* are not listed here, and setup and management of these lie in the responsibility of the DBA. The initial or extent size for the segments of the tablespaces must be set according to the default values.

Tablespace name	Initial size	Extent increment*
USERS	512M	128M
USRINDEX	512M	64M
TEMP	512M	8M
UNDO	512M	16M

* Extent size of the corresponding data files for the auto extent.



It is recommended to use the following storage options for user defined tablespaces:

- local management
- autoextent|

4.4.2.8 Redo log files

The recommended initial redo log file size is 128 MB.

It is recommended to create at least 3 redo log groups.

i The size and number of redo log files might need to be adapted during the database life time e.g. for performance reasons.

4.4.2.9 Database statistics

It is strongly recommended to gather workload system statistics during a period of average database load and to regularly update objects statistics using the Oracle dbms_stats package, if not yet done by the default automatic system task *GATHER_STATS_JOB*.

4.4.3 Oracle user requirements

4.4.3.1 General

All PAS-X users will be set up and configured during PAS-X server system setup. The following statements are for information purposes only.

4.4.3.2 Default settings

The following table lists the default PAS-X Oracle database users:

PAS-X Oracle username	Default password	Default tablespace	Additional tablespaces	Default TEMP tablespace	Password lifetime
PASX	****	USERS	USRINDEX	TEMP	Unlimited

i Each user should be granted "quota unlimited" for the default and the additional tablespaces.

4.4.3.3 Required PAS-X privileges

- ALTER SESSION
- CREATE SESSION
- CREATE PROCEDURE
- CREATE SEQUENCE
- CREATE SYNONYM
- CREATE TABLE
- CREATE TRIGGER
- CREATE VIEW

i The required privileges may be grouped and granted to an Oracle role.

4.4.3.4 Required SYS privileges for PASX

The following table lists the required SYS privileges that must be granted by the Oracle SYS user to the PAS-X Oracle users *PASX*:

- EXECUTE ON DBMS_ALERT

i SYS privileges cannot be granted to an Oracle role and therefore must be granted directly to *PASX*.

4.4.3.5 Extended privileges for maintenance and troubleshooting

A dedicated Körber Pharma Software maintenance user is not created as part of the server system setup.

It is recommended to create such a user to analyze a problem in the PAS-X database and to be able to get all required information Körber Pharma Software will need. Either:

- the password of the database user *SYSTEM/SYS*
– or –
- the username/password of a dedicated Körber Pharma Software maintenance user on the database who has been granted the *SELECT_CATALOG_ROLE* and *EXECUTE_CATALOG_ROLE* system roles

4.4.4 PostgreSQL software requirements

4.4.4.1 PostgreSQL version

See section: [PAS-X runtime configuration/ Server](#)

4.4.4.2 PostgreSQL software components

The PostgreSQL RDBMS can be used on any kind of operating system or prebuild service as long as the requirements for the version and the extensions can be fulfilled.

4.4.5 PostgreSQL database requirements

4.4.5.1 General

In PostgreSQL, a schema is a namespace that contains named database objects. PAS-X requires a single schema on the database. This schema has to be prebuilt by the customer. PAS-X will use a single schema to store all relevant objects like tables and views.

i PAS-X requires the database schema name and the database user to be named identical.

4.4.5.2 PostgreSQL database components

PAS-X will not require any additional extension in the PostgreSQL database to operate, but we recommend installing the following extensions to optimize the monitoring of the database:

- pg_prewarm
- pg_stat_statements

4.4.5.3 Initialization parameters


The following tables describe the basic PostgreSQL instance settings that are used to set up the system initially.




4.4.5.3.1 Compiling parameters

Parameter	Value
SEGSIZE	2
BLOCKSIZE	8
openssl	true

4.4.5.3.2 Initialization parameters

The following table listed recommended values.

Parameter	Value	Mandatory
effective_cache_size	6GB  75% of the available memory.	
huge_pages	on	
log_autovacuum_min_duration	60s	
log_checkpoints	on	
log_connections	off	
log_directory	pg_log	
log_disconnections	off	
log_duration	off	

Parameter	Value	Mandatory
log_filename	postgresql-%b.log	
log_line_prefix	%m - %l - %p - %h - %u@%d - %x	
log_lock_waits	on	
log_min_duration_statement	10s	
log_min_error_statement	NOTICE	
log_min_messages	WARNING	
log_rotation_age	1440	
log_statement	ddl	
log_temp_files	0	
log_timezone	 Locale, e.g.: Europe/Berlin or 'GMT'	
log_truncate_on_rotation	on	
logging_collector	on	
maintenance_work_mem	64MB	
max_connections	300	yes
max_files_per_process	2000	yes
max_locks_per_transaction	200	yes
max_prepared_transactions	64	yes
shared_buffers	2GB  25% to 40% of the available memory.	
shared_preload_libraries	pg_stat_statements,pgrowlocks	
TimeZone	 Locale, e.g.: 'GMT'	
track_activity_query_size	2048	
work_mem	8MB	

4.4.5.4 Encryption

To enable SSL encryption of the PostgreSQL database traffic and authentication, the database must be prepared to use hostssl.


Variable	Values
ssl	on
hostssl	 hostssl configuration in the <i>pg_hba.conf</i> file.

4.4.6 PostgreSQL database prerequisites

PAS-X MES requires a prepared PostgreSQL database for the software deployment.

4.4.6.1 Creating roles and database

On the instance level as a superuser, create the roles and database as stated below.

-  • "{PASX}" is the placeholder for the PAS-X technical user database role
- "{MONITORING}" is the placeholder for the PAS-X Monitoring technical database role
- "{PASXDB}" is the placeholder for the new created PAS-X application database

Role and schema must have the same name!

All placeholders can be defined at your own discretion.

Create the following roles:

Roles
"{PASX}"
"{MONITORING}"

Create the following database:

Database
"{PASXDB}"

4.4.6.2 Creating objects and grants

On the database level ("{PASXDB}") as the created "{PASX}" user, create the following objects and grants:

Create the following objects:

Object Type	Object Name	Example statement
SCHEMA	"{PASX}"	CREATE SCHEMA IF NOT EXISTS "{PASX}"
SCHEMA	"{MONITORING}"	CREATE SCHEMA IF NOT EXISTS "{MONITORING}"

Create the following privileges:

Grant Privilege
GRANT USAGE ON SCHEMA "{PASX}" TO "{MONITORING}"
GRANT SELECT ON ALL TABLES IN SCHEMA "{PASX}" TO "{MONITORING}"
GRANT SELECT ON ALL SEQUENCES IN SCHEMA "{PASX}" TO "{MONITORING}"
GRANT USAGE ON SCHEMA "{MONITORING}" TO "{MONITORING}"
GRANT SELECT ON ALL TABLES IN SCHEMA "{MONITORING}" TO "{MONITORING}"
GRANT SELECT ON ALL SEQUENCES IN SCHEMA "{MONITORING}" TO "{MONITORING}"
GRANT PG_MONITOR TO "{MONITORING}"

Change the following privileges:

Default Privilege
ALTER DEFAULT PRIVILEGES FOR ROLE "{PASX}" IN SCHEMA "{PASX}" GRANT SELECT ON TABLES TO "{MONITORING}"
ALTER DEFAULT PRIVILEGES FOR ROLE "{PASX}" IN SCHEMA "{PASX}" GRANT SELECT ON SEQUENCES TO "{MONITORING}"
ALTER DEFAULT PRIVILEGES FOR ROLE "{MONITORING}" IN SCHEMA "{MONITORING}" GRANT SELECT ON TABLES TO "{MONITORING}"
ALTER DEFAULT PRIVILEGES FOR ROLE "{MONITORING}" IN SCHEMA "{MONITORING}" GRANT SELECT ON SEQUENCES TO "{MONITORING}"

It is recommended to drop the PUBLIC schema:

Security
DROP schema PUBLIC

4.5 ERP Integration

Integration with ERP system is possible.

- i** If the ERP system serves over HTTPs, the root certificate for the ERP system is required, unless this root CA is a commonly trusted CA.

Supported message formats are:

4.5.1 XML IDoc

IDoc, short for Intermediate Document, is an SAP document format for business transaction data transfers.

This format is supported out of the box by PAS-X.

Integration with non-SAP systems is possible if they support XML IDoc but this might require to operate additional middlewares.

4.5.2 SAP RFC

Integration with the SAP system is possible via the SAP RFC interface.

Integration requires availability of SAP Java Connector libraries (which are to be provided by the customer) during deployment:

- SAP Java Connector (*sapjco3.jar* and *libsapjco3.so*)
- SAP Java IDoc Class Library (*sapidoc3.jar*)

For detailed information regarding library versions see section: [PAS-X runtime configuration](#).

4.6 Fonts

The default reports and labels provided with PAS-X are using the Liberation True Type font.

This font is included with the relevant PAS-X server components.

i Custom reports / labels / fonts

- Customized reports and labels based on any other True Type font can be used. Keep in mind that such a custom font is **not** part of PAS-X and is to be provided and licensed individually.
- Customized reports and labels as well as custom fonts are to be provided as a ZIP archive and will be applied to PAS-X during deployment.

4.7 Operating System

Linux

Linux is required as operating system for deploying and running PAS-X.

Microsoft Windows

Microsoft Windows is required as operating system for

- running the PAS-X Client.
- running integration with *Level 2* and *LIMS/CAPA* Systems.

Extended privileges for maintenance and troubleshooting

The Körber Pharma Software Service Desk might be asked to analyze a problem in the PAS-X database and thus has to be able to get access to all the required information to complete the service request. Körber Pharma Software will need either:

- the password of the database user *SYSTEM/SYS*
– or –
- the user name/password of a dedicated Körber Pharma Software maintenance user who has been granted the *SELECT_CATALOG_ROLE* and *EXECUTE_CATALOG_ROLE* system roles in the database.

Local Security Policy for Microsoft Windows

Set *Local Security Policy\Local Policies\Security Option\System cryptography*: "Use FIPS compliant algorithms for encryption, hashing, and signing" to **disabled**.

4.8 Password Encryption

PAS-X MES requires some passwords to be configured in an encrypted form. To encrypt these, an encryption utility is provided with the System Manager bundle. This utility will encrypt the single values in the required form and also encrypt their whole configuration file.

See the "System Manager" system manual for details.

4.8.1 Restricted characters for configuration property values.

Note that passwords and other property values may not contain the '\$' character. '\$' is interpreted as indicating a reference.

4.9 PAS-X Client

The PAS-X client must be started using the Web Start utility, which also requires a Java Runtime Environment to operate. For more details, see section: [Java Runtime Environment \(JRE\)](#).

Web Start can be utilized directly from the command line or indirectly via a web browser. For more details, see section: [Web Start \(IcedTea-Web\)](#).

You may also use Citrix application publishing with a prepared Web Start Citrix XenApp farm server. For more details, see section: [Citrix Terminal](#).

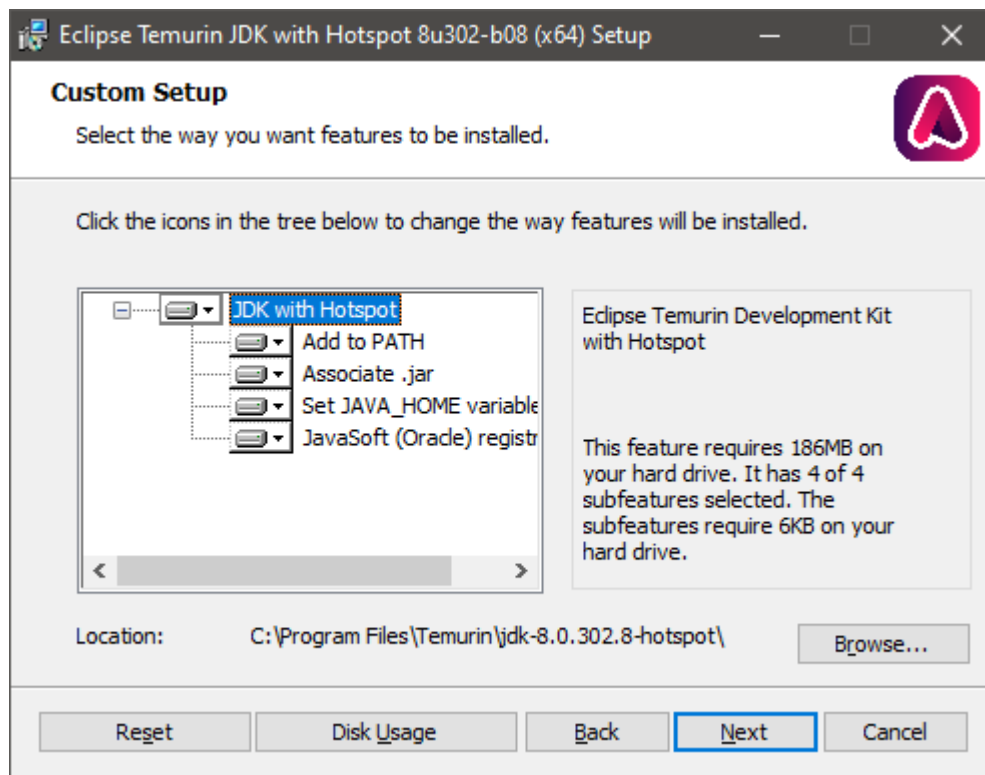
4.9.1 Java Runtime Environment (JRE)

i For the supported JRE version, see section: [PAS-X runtime configuration](#).

4.9.1.1 JRE Installation

There are several distributions of OpenJDK JRE freely available on the internet. One of the most widely used is available at <https://adoptium.net>. We recommend using the installer of this distribution.

1. Download the installer which matches the supported version (see section: [PAS-X runtime configuration](#)) and which is suitable for your hardware platform and operating system.
2. Follow the installation procedure as usual. Example:



i The IcedTea-Web utility has to be installed separately. See section: [IcedTea-Web Installation](#).

4.9.2 Web Start (IcedTea-Web)

PAS-X uses the Java Web Start technology to start the PAS-X client, hosted on a remote server, directly from a web browser. This reduces the necessary client software stack to a web browser, a JVM – a Java Virtual Machine, part of the Java Runtime Edition (JRE) – and *IcedTea-Web* (the Java Web Start launcher), and it obviates the need to pre-install and update the PAS-X client on local workstations.

- i • To directly retrieve or update a software release from a remote host, to verify the integrity of the package and to start the application, Java Web Start defines the Java Network Launch Protocol (JNLP).
- IcedTea-Web is an open source implementation of a client to that protocol. It requires at least a *.jnlp* file as a parameter to download the corresponding software package.
- A PAS-X Web Start Client needs to meet the requirements for memory and CPU cores to execute the PAS-X client application.
 - i These requirements depend on the use cases of PAS-X as well as on the selected zone and sizing model of your system. Please contact Körber Pharma Software if you need more information about system sizing and the related requirement impacts.
- For supported web browsers and requirements, see section: [PAS-X runtime configuration](#).

There are two possible ways to start the PAS-X client via Web Start:

1. Directly via command line or shortcut (recommended):
 - a. Create a shortcut to `<IcedTea-Web Installation Path>/WebStart/bin/javaws.exe https://<PAS-X System Host>/pasxclient/startpasx.jnlp`.
 - b. Execute the shortcut.
 - ▶ The PAS-X client start file (*startpasx.jnlp*) is downloaded and the PAS-X client is started.
2. Indirectly via web browser:
 - a. Enter the following URL: `https://<PAS-X System Host>/pasxclient`.
 - b. Click **Start PAS-X**:



- ▶ The web browser will download the PAS-X client start file (*startpasx.jnlp*).
- If the web browser is configured to open a *.jnlp* file type directly with IcedTea-Web (*javaws.exe*; see section: [IcedTea-Web Configuration](#)), the PAS-X client will automatically be started.
- Depending on the web browser type and its configuration, the user might need to acknowledge an additional warning before the PAS-X client can be started.

If the *.jnlp* file type action is not assigned, the user needs to start the PAS-X client manually by executing the downloaded *startpasx.jnlp* file.

4.9.2.1 IcedTea-Web Installation

The IcedTea-Web utility has to be installed separately as it no longer a feature of the JRE. It still is maintained and supplied by the AdoptOpenJDK project.


1. From the project homepage at <https://adoptopenjdk.net/icedtea-web.html>, download the installer which matches the supported version and which is suitable for your hardware platform and operating system (see section: [PAS-X runtime configuration](#)).
2. Run the installer. There are no options except for the installation location.

4.9.2.2 IcedTea-Web Configuration

After the installation of IcedTea-Web, you will find the following Windows executables in the */bin* subdirectory within the installation directory of IcedTea-Web :

1. *itweb-settings.exe* allows you to configure your IcedTea-Web installation - see below.
2. *javaws.exe* allows you to directly start an application by supplying the corresponding JNLP file. See section: [Web Start \(IcedTea-Web\)](#).
3. *policyeditor.exe* allows you to elaborate security policies from permissions for Java code execution.

4.9.2.2.1 Configuration of IcedTea-Web

 The IcedTea-Web utility can be configured with *itweb-settings.exe* located in the */bin* folder of the IcedTea-Web installation.

1. On the configuration page **JVM settings**, in the field "Set JVM for IcedTea-Web", verify that the path to the JRE installation is correct.
The JVM setting can be used to force IceTea-Web and thereby the PAS-X client to use a specific Java version beside the default Java version of the system.
2. In case you need to take a special web proxy into account, this should be configured on the configuration page **Network**.
3. In case you want applications to be able to create desktop shortcuts, this can be enabled on the configuration page **Desktop Integration**.
4. In case certain certificates have to be made known to IcedTea-Web, this must be done on the configuration page **Certificates**.
5. IcedTea-Web warning dialogs on PAS-X startup can be avoided or suppressed:
 - a. By setting specific IcedTea-Web configuration options (e.g. by suppressing the creation of desktop shortcuts on the configuration page **Desktop Integration**)
 - b. By providing the relevant SSL certificates to IcedTea-Web on the configuration page **Certificates**.

4.9.2.2.2 IcedTea-Web Association with JNLP files

**.jnlp* files should have become associated with *javaws.exe* in the */bin* folder of the IcedTea-Web installation during installation. This will also imply that links to *.jnlp* files, on which you click in your browser, will be opened by IcedTea-Web. If that is not the case, there are only a few ways to rectify this manually.

One way is to display the **Properties** dialog for a *.jnlp* file (by selecting *Properties* from the context menu of the Windows Explorer for that file) and change the "Opens with..." association right on top of the first page to *javaws.exe* in the */bin* folder of the *IcedTea-Web* installation.

4.9.2.3 Setting the terminal ID for Web Start

The terminal ID is used to identify a terminal. This defines in particular which orders of production units are visible on that terminal.

If PAS-X is configured to use the external authentication interface (e.g. using card readers), the terminal ID is also used when communicating with the external authentication system.

By default, a terminal uses its client host name as its ID and this is sufficient in most cases.

Changing the default behavior

If it is necessary to change the terminal ID for a client, the following can be done:

1. Download and save the *.jnlp* file from the URL that you use to start the client (see section: [Web Start \(IcedTea-Web\)](#)).
 - a. On the terminal you want to configure, navigate to *https://<PAS-X System Host>/pasxclient*.
 - b. Right-click on the **Start PAS-X** button and select "Save link as".
 - c. Select a location to save the file and confirm.
2. Edit the file:
 - a. Open the file in a text editor.
 - b. Delete *href="startpasx.jnlp"* from the following line:

startpasx.jnlp

```
<jnlp spec="1.0+" codebase="https://<PAS-X System Host>/pasxclient"
href="startpasx.jnlp">
```

- c. Add a new line with the following content below the other similar looking "property" elements:

startpasx.jnlp

```
<property name="jnlp.pass.PASX_V3_TERMINAL_ID" value="<Your terminal ID>" />
```

- d. Save the file on the terminal.

You can now use this file to start PAS-X. The terminal you defined will be used for the started client.

To verify that the terminal ID was taken over correctly, select **Help > About** in the menu of PAS-X to open the "System Information" dialog. The **Client info** section displays the terminal ID.

4.9.3 Web Browser

PAS-X is based on a hybrid application UI approach, composed of desktop application dialogs (classic application) on the one side and web application dialogs (web application) running in a web browser on the other side.

This section therefore highlights the main aspects of the PAS-X web browser integration with a special focus on the supported browsers and their configuration.

4.9.3.1 Web Browser Support

During the FAT, Körber Pharma Software verifies the compatibility of PAS-X to run under a specific version of each supported web browser type.

- i For supported web browsers and versions, see section: [PAS-X runtime configuration](#).
 - Please note that Körber Pharma Software does not verify or guarantee any backward or forward compatibility to any other than the stated browser version. In this context, see also section: [Web Browser Updates](#).
 - Please note that PAS-X will use the default browser of the operating system.

Whenever providing a new version of PAS-X, Körber Pharma Software decides to select and verify new versions of each supported web browser type. Körber Pharma Software thereby aims to use the latest ESR version of Mozilla Firefox and the latest stable version of Google Chrome.

- i Please note that PAS-X patch updates and PAS-X hot fixes do not require any web browser updates, except cases where a fix is directly related to a specific web browser version.

4.9.3.2 Web Browser Configuration

Depending on the PAS-X deployment characteristics, there are different possibilities to configure the web browser locally or centrally. A central web browser configuration is possible by using Windows group policies (e.g. <https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy-windows>) or by using Citrix (or similar environments). The central administration of web browser settings allows applying standardized environments to a group of users and computers in order to achieve more efficient configuration management.

It might be helpful to reduce the complexity of the web browser for the operators by disabling some of the browser functionality. Examples:

- Disable the menu bar
- Disable the bookmarks toolbar
- Remove the address bar
- Reduce the browser to use one browser tab only. See section: [Reducing the Web Browser to Use One Browser Tab Only](#).

4.9.3.2.1 Reducing the Web Browser to Use One Browser Tab Only

By default, the supported browser types open each new PAS-X web dialog in a separate browser tab. This can lead to a confusing number of simultaneously open browser tabs that make it hard to find back to the right tab when needed.

In order to obviate this situation, you can configure the browser to open a new link (PAS-X dialog) in the current open tab/window. Examples:

Mozilla Firefox

In order to configure Mozilla Firefox to open a new link (PAS-X dialog) in the current open tab/window, start the Firefox configuration editor by entering "about:config" in the address bar and change the setting of "browser.link.open_newwindow" to "1":



For further information about Firefox Configuration Editor, see: <https://support.mozilla.org/en-US/kb/about-config-editor-firefox>.

For deploying Firefox in an enterprise environment, see: <https://support.mozilla.org/bm/products/firefox-enterprise/deploy-firefox-for-enterprise>.

Google Chrome

Google Chrome does not support opening a link (PAS-X dialog) in the current open tab/window directly, but this can for example be done by using the Google Chrome extension "xTab".

Configure "xTab" to *tab-limit = 1* and the extended setting to *reuse existing tab*.

i Please note that this setting will also force that pages which are triggered by a user request (e.g. by pressing "+" in the tab bar) are opened in the same browser tab/window.

i Document viewer interfering PAS-X Client view

Using a web browser as default application for certain document types, e.g. PDF, might interfere with the PAS-X client views.

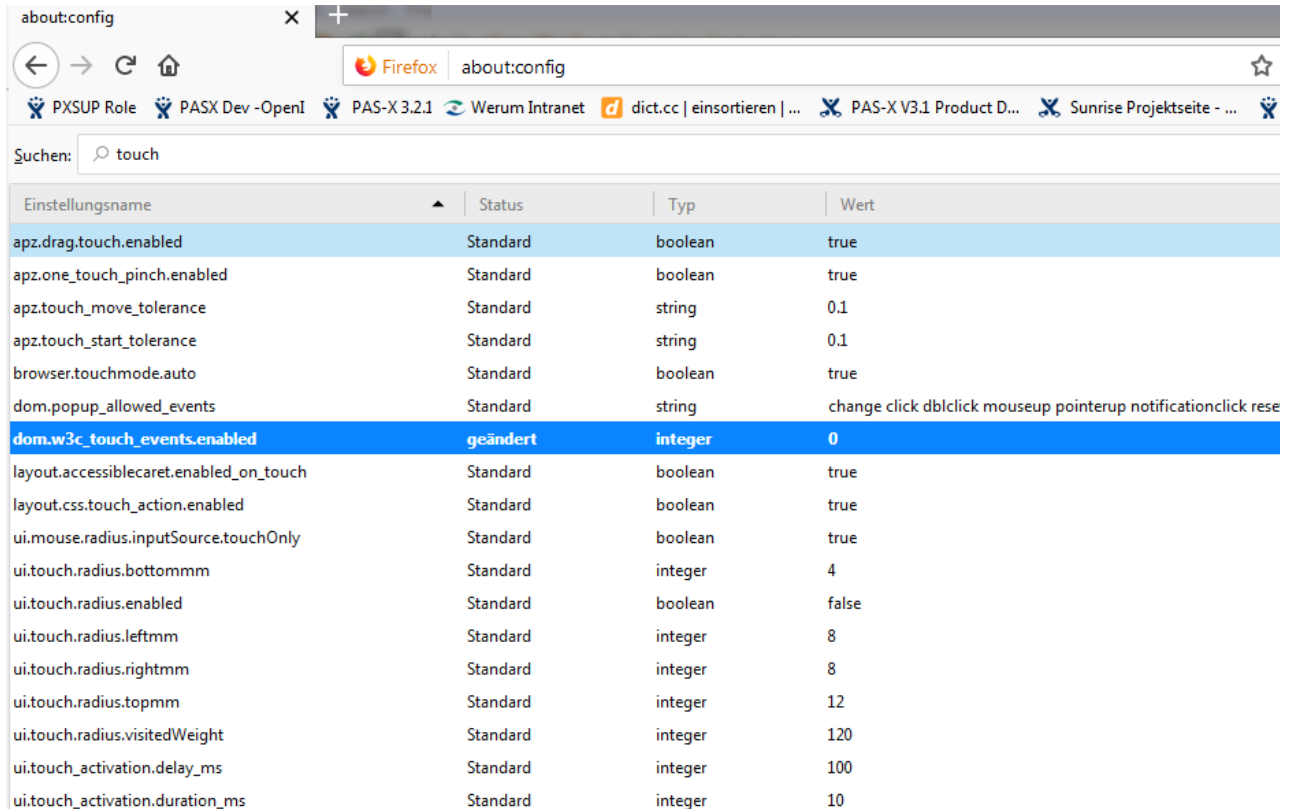
In such a scenario, viewing a document might use the active browser tab showing the PAS-X client views.

It is not recommended to use the web browser in *One Tab* mode when using the browser as document viewer.

4.9.3.2.2 Disabling Touch Input

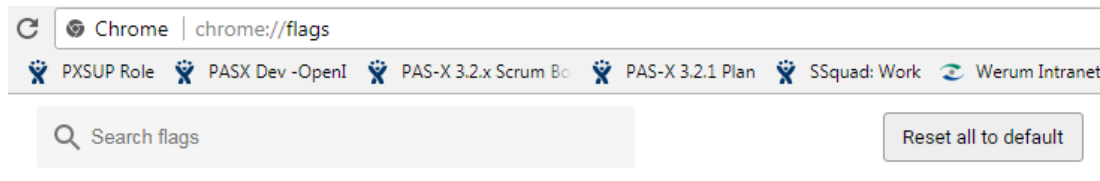
Disable the touch input for the browser to prevent problems when selecting rows of PAS-X web dialogs.
Examples:

Mozilla Firefox



Einstellungsname	Status	Typ	Wert
apz.drag.touch.enabled	Standard	boolean	true
apz.one_touch_pinch.enabled	Standard	boolean	true
apz.touch_move_tolerance	Standard	string	0.1
apz.touch_start_tolerance	Standard	string	0.1
browser.touchmode.auto	Standard	boolean	true
dom.popup_allowed_events	Standard	string	change click dblclick mouseup pointerup notificationclick rese
dom.w3c_touch_events.enabled	geändert	integer	0
layout.accessiblecaret.enabled_on_touch	Standard	boolean	true
layout.css.touch_action.enabled	Standard	boolean	true
ui.mouse.radius.inputSource.touchOnly	Standard	boolean	true
ui.touch.radius.bottommm	Standard	integer	4
ui.touch.radius.enabled	Standard	boolean	false
ui.touch.radius.leftmm	Standard	integer	8
ui.touch.radius.rightmm	Standard	integer	8
ui.touch.radius.topmm	Standard	integer	12
ui.touch.radius.visitedWeight	Standard	integer	120
ui.touch_activation.delay_ms	Standard	integer	100
ui.touch_activation.duration_ms	Standard	integer	10

Google Chrome



Experiments

64.0.3282.119

WARNING: EXPERIMENTAL FEATURES AHEAD! By enabling these features, you could lose browser data or compromise your security or privacy. Enabled features apply to all users of this browser.

Interested in cool new Chrome features? Try our [beta channel](#).

Available

Unavailable

Touch Events API

Force **Touch** Events API feature detection to always be enabled or disabled, or to be enabled when a **touch** screen is detected on startup (Automatic, the default). – Mac, Windows, Linux, Chrome OS

[#touch-events](#)

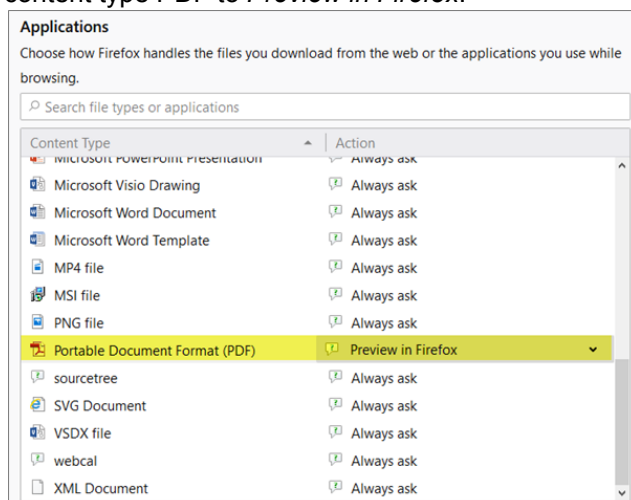
Disabled

4.9.3.2.3 Using the Internal PDF Viewer of the Web Browser

Web browser can be configured to use the internal PDF viewer of the browser. This configuration will force PAS-X to open a PDF file – like the BRR – in a browser window instead of opening it in a separate PDF viewer application window. Examples:

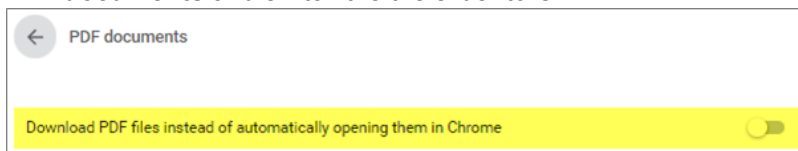
Mozilla Firefox

In order to show PDF files in Mozilla Firefox, select **Options > Applications** and set the action for the content type PDF to *Preview in Firefox*:



Google Chrome

In order to show PDF files in Google Chrome, select **Settings > Advanced > Privacy and security > Site > PDF documents** and switch the the slider to OFF:



4.9.3.2.4 Disabling development tools and extensions

The browser's developer tools allow a user to modify the content of a page or its cookies. Browser extensions provide even more possibilities.

You may want to limit the users' ability to perform such changes.

Mozilla Firefox

Firefox can be configured using policies. <https://github.com/mozilla/policy-templates/releases> describes which policies can be used for each version of Firefox.

Use "DisableDeveloperTools" to disable the developer tools. You can use the policy called "Extensions" to control which extensions (if any) should be installed.

The policies are set in different ways depending on the operating system. For more information, see <https://support.mozilla.org/en-US/products/firefox-enterprise/policies-customization-enterprise/policies-overview-enterprise>

Google Chrome

Chrome is configured via policies, too. For more information, see <https://cloud.google.com/docs/chrome-enterprise/policies/>

Use "DeveloperToolsAvailability" to disable the developer tools. Policies for extensions can control which extensions are installed: <https://cloud.google.com/docs/chrome-enterprise/policies/atomic-groups/#extensions>

4.9.3.3 Web Browser Navigation

The "PAS-X" reference manual describes how to navigate in the classic application, in the web application and between both application types and dialog types. See section: "General GUI description".

4.9.3.4 Web Browser Add-ons and Extensions

Körber Pharma Software does not verify any specific browser add-ons or extensions during FAT. If, however, the support of a specific browser add-on or extension is required, Körber Pharma Software offers the service to facilitate the support via customization for a specific customer project.

4.9.3.5 Web Browser Security

PAS-X services are configured to serve over HTTPS by default. In this case, a root CA certificate that vouches for the certificates used for the SSL/TLS handshake must be accepted as trusted root CA by the browsers in order to properly work with the PAS-X services.

4.9.3.6 Web Browser Updates

During the FAT, Körber Pharma Software verifies the compatibility of PAS-X to run under a specific version of each supported web browser type.

 Deactivate the automatic update mechanism of the web browser.

4.9.4 Citrix Terminal

Before publishing the PAS-X Client application, the PAS-X Web Start Client must be made available on every Citrix XenApp farm server.

This can be done manually by using the command line integration of Web Start. See section: [Web Start \(IcedTea-Web\)](#).

- **Connection Limits:** The allowed connections per user should be unlimited.
- **Session Reliability:** Session reliability must be enabled.
- **Requirements on the Citrix XenApp farm:** Web browser.
- **Session Reconnection Policy:** To ensure, that the terminal ID of the session always corresponds to the correct physical terminal device, change the session reconnection policy to *SameEndpointOnly*.

4.9.5 Encrypted Client Communication

With Java, it is possible to employ the built-in trust store of the operating system or a trust store which is specific to the used Java Runtime Environment. If the certificate used by the services and the Wildfly server is signed by a trusted Certificate Authority, the certificate of that trusted CA is likely to be already contained in the corresponding trust store of the client operating system. Therefore, it is not necessary to specifically import it into the one of the JREs.


For Windows operating systems, the relevant storage of certificates will be the Windows Certificate Store (Windows-Root trust store).

4.10 PDF/A conversion / Ghostscript

Archived BRRs and labels can be converted to PDF/A by the application server. For this, Ghostscript has to be available as binary during deployment. The Ghostscript version must be equal to or higher than the version mentioned in [PAS-X runtime configuration / Server](#).

GPL prohibits distributing Ghostscript with the existing deployment, and therefore it has to be provided by the customer.

4.11 Time Zone

 PAS-X requires that all infrastructure elements, the belonging DBMS server and the NTP server are configured to run on UTC.

In order to have the correct time zone assigned to events taking place in PAS-X, a time zone must be configured for deployment and entered in the PAS-X configuration data. The time zone information will be used to render the correct date and time information together with the configured date and time formats. The system configuration offers options for localization where the required settings can be made.

! Should the entry be missing, a standard time zone (Europe/Berlin) will be set and errors would occur in the representation and processing of dates as a result of using a different time zone.

The currently used database time zone is set automatically for this PAS-X configuration data during system setup.

1. Start PAS-X server-side components.
2. Start the PAS-X client and open the "Control data" dialog.
3. Insert/update a data record with the following attributes:

Attribute key	Dimension key	Value
<i>System.Formats.Date.TimeZone4Date</i>	<i>default</i>	<p><TZ> Replace <TZ> with a suitable time zone name.</p> <p>! This value must be set to the time zone chosen in PAS-X deployment. It must not be changed after production or batch data have been acquired.</p> <p>i The list of the time zone names is available from the IANA on: http://www.iana.org/time-zones</p>

5 Appendix

This section describes the required hardware specifications.

5.1 Supporting Infrastructure Components

The following components are part of the IT infrastructure:

- Network
- DNS
- Firewall
- Virus Protection Software
- Active Directory Services (e.g. ADDS, LDAP)
- Timeserver
- Time synchronization service to synchronize system time between the different components
- Uninterruptible Power Supply (UPS)
- Backup & Recovery
- Archive Server

5.2 Systems Sizing Introduction

Get in contact with Körber Pharma Software for detailed information on infrastructure dimensioning.

5.3 Availability Options

Basic availability will be ensured by deploying PAS-X on Docker in Swarm mode.

The following additional availability options can be provided by the customer.

- **Database**
 - Database Replication technology
- **Storage**
 - Storage (SAN) Mirroring
- **Virtualization**
 - Virtualization technologies (e.g. VMWare HA-option)
 - Citrix XenApp

5.4 Production Network

For wired client connections, the production network infrastructure must be capable of operating at a minimum speed of 1 Gbit/s.

For the production network, package latency < 1ms is recommended.

5.5 Virtualization Statement

- Körber Pharma Software does platform releases for PAS-X MES for selected client operating systems.
- The VMWare hypervisor (or any other bare-metal hypervisor) adds an additional layer between the physical hardware and the operating system.
- The hypervisor has to be released for "productive use" by the vendor.

5.6 Recommended Monitoring Spots for PAS-X Systems

The objective of system monitoring is to check the health status of the systems during trial operations and/or PQs. Its objective is not to make the system's runtime behavior more efficient (profiling).

In the following, methods and tools are listed that can be used for system monitoring of hardware utilization and base software. The data that has to be monitored is briefly outlined. Apart from performance data, system monitoring also supports troubleshooting performance issues.

The system is considered to be overloaded when certain thresholds are permanently exceeded. However, single performance peaks occurring when applications are started cannot be seen as a system overload.

The following items should be monitored:

- **Server**
 - CPU: utilization
 - Main memory: utilization, failure
 - Hard disks: utilization, failure
 - Network boards: utilization, latency times, availability
 - Event logs
 - **Network**
 - Overall network, sub networks, single components: throughput
 - Router: utilization
 - Switch: utilization
 - **Database**
 - Table spaces: growth
 - Data files: growth, corrupted data blocks
 - Trace files: error messages
 - Backup log files: existence, error messages
- System monitoring can be divided into two categories: system analysis for the short-term diagnosis of the current resource utilization and system analysis for the long-term acquisition of the resource usage.
- **Container Runtime (Docker)**
 - Docker Stats
 - Volume growth
 - **Tools for short-term problem analysis**
 - Windows: Task Manager, Performance Monitor (operating system components); administrative tools from SysInternals such as FileMon, Pmon and Process Explorer; Windows Server Resource Kit

- Unix system standard tools for network analysis (netstat, top, iostat and tcpdump etc.)
- System programs for logging event messages from system services and kernel events
- Switch/router monitoring and management tools for error situation detection and for throughput monitoring (collision detection)
- **Tools for long-term system monitoring (incl. alert management)**
 - PAS-X monitoring
 - Monitoring tools such as Nagios (UNIX program with plugins for Windows systems), HP OpenView, Tivoli and WhatsUp Gold etc.
 - Solutions provided by the system manufacturer, such as HP, for monitoring their server systems
 - Trace tools and log analyzer such as BigSister for monitoring and analyzing alert and log files
- **Virtual Infrastructure**
 - Standard tools for resource allocation monitoring (e.g. esxtop)

5.7 Network Communication

This section lists all default ports.

5.7.1 Network Ports for Docker Swarm

5.7.1.1 Docker Swarm Ports

Source	Target	Protocol/Service	Server IP Port (standard)	Comment
Management Host	Clustered Container Hosts	TCP	22 (or 2375), 2377	Remote swarm administration, deployments 2375 would be used to access docker socket unsecured without ssh
Clustered Container Hosts	Clustered Container Hosts	TCP / UDP	7946	Docker swarm internal communication
Clustered Container Hosts	Clustered Container Hosts	UDP	4789	Docker swarm overlay networking Ensure ip protocol 50 (ESP) traffic is allowed (IPSec for encrypted overlay network)

5.7.1.2 PAS-X Ports

Source	Target	Protocol	IP Port	Comment
Client	Clustered Container Hosts	RMI via TLS	443/tcp	PAS-X Client communication with PAS-X server components
Client	Clustered Container Hosts	HTTPS	443/tcp	PAS-X web based Client communication with PAS-X server components
Clustered Container Hosts	CUPS	CUPS IPP	631/tcp udp	Communication with CUPS for printing capabilities
Interfacing Hosts	Clustered Container Hosts	AMQP via TLS	25671/tcp	RabbitMQ SSL communication
Client	Clustered Container Hosts	HTTPS	443/tcp	PAS-X client download
Clustered Container Hosts	Oracle Database	TCP	1521/tcp	Database related communication on using Oracle database
Clustered Container Hosts	PostgreSQL Database	TCP	5432/tcp	Database related communication on using PostgreSQL database
Clustered Container Hosts	NFS	NFSv4	2049/tcp udp	Communication from Clustered Container Hosts to the NFS service



Source	Target	Protocol	IP Port	Comment
"Each source"	Clustered Container Hosts (Message Broker)	AMQP	5672/tcp	Direct communication with message broker
			443/tcp	RabbitMQ management interface

5.7.1.3 URLs

Port	URL path	Description
443	/pasxhelp	Web UI for PAS-X Online Help
443 (15672) 25672 (5672)	/rabbitmq/ / / /	RabbitMQ Management Interface unsecured RabbitMQ Management Interface (exposed with activated option <code>rabbitmq-expose-unencrypted-ports</code>) Communication with RabbitMQ (AMQPS) (port is configurable) Communication with RabbitMQ (AMQP) (port is configurable, exposed with activated option <code>rabbitmq-expose-unencrypted-ports</code>)
80		Redirect to 443
443	/dashboard/	Proxy dashboard
443	/ping	Health check endpoint.
443	/auda /auda-management	Access to <i>PAS-X Authentication Adapter</i> . Access to the corresponding monitoring endpoint.
443	/central /pasxclient	Access to the <i>PAS-X Central Service</i> . Access to the PAS-X Client Download page.
443	/cockpit /cockpit-management	Access to the <i>PAS-X Cockpit Service</i> . Access to the corresponding monitoring endpoint.
443	/configservice /configservice-management	Access to the <i>PAS-X Configuration Service</i> . Access to the corresponding monitoring endpoint.
443	/edw /edw-management	Access to the <i>PAS-X EDW Service</i> . Access to the corresponding monitoring endpoint.
443	/equipment /equipment-management	Access to the <i>PAS-X Equipment Service</i> . Access to the corresponding monitoring endpoint.
443	/execution /execution-management	Access to the <i>PAS-X Execution Service</i> . Access to the corresponding monitoring endpoint.

Port	URL path	Description
443	/importexport /importexport-management	Access to the <i>PAS-X Import - Export Service</i> . Access to the corresponding monitoring endpoint.
443	/label-printing-management	Access to monitoring endpoint of <i>PAS-X Printing Service</i> for labels
443	/messagemonitoring /messagemonitoring-management	Access to the <i>PAS-X Message Monitoring Service</i> . Access to the corresponding monitoring endpoint.
443	/msi /msi-management	Access to the <i>PAS-X MSI Service</i> . Access to the corresponding monitoring endpoint.
443	/nose /nose-management	Access to the <i>PAS-X notification Service</i> . Access to the corresponding monitoring endpoint.
443	/replenishment /replenishment-management	Access to the <i>PAS-X Replenishment Service</i> . Access to the corresponding monitoring endpoint.
443	/report-printing-management	Access to monitoring endpoint of <i>PAS-X Printing Service</i> for reports
443	/scaleservice /scaleservice-management	Access to the <i>PAS-X Scale Service</i> . Access to the corresponding monitoring endpoint.
443	/storagetracking /storagetracking-management	Access to the <i>PAS-X Storage Tracking Service</i> . Access to the corresponding monitoring endpoint.
443	/task /task-management	Access to the <i>PAS-X Task Service</i> . Access to the corresponding monitoring endpoint.
443	/pasx /uia-management	Access to the <i>PAS-X Web Client</i> . Access to the corresponding monitoring endpoint.
443 (9001)	/wei /wei-management	Access to the <i>PAS-X WEI Service (XML)</i> . (Insecure access with activated option <i>wei-expose-unencrypted-ports</i> , port is configurable and defaults to 9001.) Access to the corresponding monitoring endpoint.
443	/weimonitoring /weimonitoring-management	Access to the <i>PAS-X WEI Monitoring Service</i> . Access to the corresponding monitoring endpoint.

Port	URL path	Description
443	/weirfc /weirfc-management	Access to the <i>PAS-X WEI Service (RFC)</i> . Access to the corresponding monitoring endpoint.
443	/wms /wms-management	Access to the <i>PAS-X WMS Service</i> . Access to the corresponding monitoring endpoint.
443	/pasx-monitoring	Access to the <i>PAS-X Monitoring Service</i> web interface.

5.7.2 Network Ports for Kubernetes

5.7.2.1 Ingress

Path	Backend
/auda	auda-service:8080
/audapartnersimulator	audasim-service:8080
/	central-service:8080
/pasxclient	
/cockpit	cockpit-service:8080
/configservice	configservice-service:8080
/edw	edw-service:8080
/equipment	equipment-service:880
/erpsimulator	erpsimulator-service:8080
/execution	execution-service:8080
/pasxhelp	help-service:8080
/importexport	importexport-service:8080
/messagemonitoring	memo-service:8080
/msi	msi-service:8080

Path	Backend
/nose	nose-service:8080
/pasx-monitoring	pasx-monitoring-service:8080
/rabbitmq(/ \$)(.*)	rabbitmq:http-stats
/replenishment	replenishment-service:8080
/scaleservice	scls-service:8080
/storagetracking	str-service:8080
/task	task-service:8080
/pasx	uia-service:8080
/wei	wei-service:8080
/weimonitoring	weimon-service:8080
/wms	wms-service:8080

5.7.3 Citrix Ports

5.7.3.1 Citrix License Server Ports

System	Protocol	Port	Description
License Manager Daemon	TCP	27000	Handles initial point of contact for license requests (Lmadmin.exe)
Citrix Vendor Daemon	TCP	7279	Check-in/check-out of Citrix licenses (Citrix.exe)
License Management Console	TCP	8082	Web-based administration console (Lmadmin.exe)

5.7.3.2 Common Citrix Communication Ports

System	Protocol	Port	Description
Citrix Receiver	TCP	80/443	Communication with Merchandising Server
ICA / HDX	TCP	1494	Access to applications and virtual desktops
Session Reliability	TCP	2598	Access to applications and virtual desktops
IMA	TCP	2512	Independent Management Architecture (IMA)
Management Console	TCP	2513	Citrix Management Consoles

System	Protocol	Port	Description
Application / Desktop Request	TCP	80/8080/443	XML Service
STA	TCP	80/8080/443	Secure Ticketing Authority (embedded into XML Service)
XenApp: Offline Plug-in	SMB	445	Communication with Application Hub (File Server / Share)
	HTTP/S	80/443	Communication with Application Hub (Web Server / File Server / Share)
XenApp: Power & Capacity Management Agent	TCP	11168	Communication with Concentrator
XenApp: Database	TCP	1433	Microsoft SQL Server
	TCP	1434	Microsoft SQL Server. Note: Named instance connection requires UDP 1434

5.8 PAS-X runtime configuration

5.8.1 Client

The following table shows the runtime software with versions required for running the PAS-X client.

Software category	Runtime software version	Comment
PDF reader	<ul style="list-style-type: none"> Adobe PDF Reader 11.0.10 	—
Java Runtime Environment	<ul style="list-style-type: none"> Adoptium Eclipse Temurin OpenJDK JRE 8 8u332-b09 (64 Bit) IcedTea-Web 1.8.3 	—
Operating system	<ul style="list-style-type: none"> Microsoft Windows Server 2022 Standard, Version 10.0.20348 LTSC, Build 20348.169 (For centralized execution of PAS-X clients in combination with client virtualization) 	At least one operating system is needed; both are possible at the same time. <ul style="list-style-type: none"> Windows Server 2022 for VDI clients. Windows 10 for rich clients.
	<ul style="list-style-type: none"> Windows 10, Version 1809 (For running a PAS-X client without client virtualization) 	
Web browser	<ul style="list-style-type: none"> Google Chrome 109.0.5414.120 (64-Bit) and higher 	At least one web browser is needed.
	<ul style="list-style-type: none"> Mozilla Firefox 102.3.0 ESR (64-Bit) and higher 	
Virtualization server	<ul style="list-style-type: none"> XenDesktop / XenApp 7 2203 LTSR CU1 (2022 Server) and higher 	New cumulative updates (CU) can be applied.

5.8.2 Server

The following table shows the base/runtime software required for running the PAS-X Server Components.

Software category	Runtime software version	Comment
Unix Printing system	<ul style="list-style-type: none"> CUPS 2.2.7 	—

Software category	Runtime software version	Comment
Container Orchestration Platform	• Docker CE 20.10	Only one Container Orchestration Platform is required; It is not possible to use both at the same time.
	• Kubernetes API v1.24	
Deployment	<ul style="list-style-type: none"> • Helm 3.9 • kubectl 1.25 • Bash 5.0.17 	<p>Only needed if Container Orchestration Platform Kubernetes is used.</p> <p>Bash major version 5.x is required on Deployment Host.</p>
PDF/A creation	• Ghostscript 9.56.1	—
PDF/A creation / Fonts	• Ghostscript fonts 8.11	—
Relational Database Management System (RDBMS)	• Oracle 19.3.0 SE2/EE	Only one RDBMS is required; It is not possible to use both at the same time.
	• PostgreSQL 14.0	
Libraries for SAP RFC communication	<ul style="list-style-type: none"> • SAP Java Connector 3.1.4 • SAP Java IDoc Class Library 3.1.1 	Only relevant for SAP RFC communication. See also section: SAP RFC .

5.8.3 Platform Releases

Alternative platforms and their prerequisites for this PAS-X version are specified and released in the platform release documents belonging to this PAS-X version.