Installation

Informatica MDM - Product 360

Version: 10.5 HotFix 3 SP 1

Table of Contents

1 Pre-Installation Checklist 11
2 Logical Service Overview 11
3 General Communication Overview 12
4 Port Overview 13
4.1 Database 13
4.2 Server, Web and Desktop 14
4.3 Elasticsearch 15
4.4 Media Manager 15
4.5 Port range 16
4.5.1 Supplier Portal 17
5 Step by Step installation guide 18
5.1 Pre-Requisites 18
5.1.1 Pre-Requisites for Product 360 Supplier Portal 18
5.1.2 Pre-Requisites for Active Vos 18
5.1.3 Documentation 18
5.1.4 Operating system 19
5.1.4.1 Data Quality 19
5.1.5 Application and install file matrix 20
5.2 Installation of Product 360 applications 21
5.2.1 1. Installation of the Product 360 Server 21
5.2.1.1 1.1 Installation of the database 21
5.2.1.2 1.2 Installation of the Product 360 Control Center 22
5.2.1.3 1.3 Installation of Active Message Queue 22
5.2.1.4 1.4 Installation of Elasticsearch 22
5.2.1.5 1.5 Installation of the Product 360 Application server 22
5.2.2 2. Installation of the Product 360 Desktop Client 23
5.2.3 3. Installation of the Product 360 Supplier Portal 23
5.2.3.1 3.1 Installation of the database 23
5.2.3.2 3.2. Installation of Supplier Portal 23
5.2.4 4. Installation of BPM / ActiveVos 24

5.2.4.1 4.1 Installation of the database ... 24
5.2.4.2 4.2 Create a Active Vos root folder ... 24
5.2.4.3 4.3 Installation of Tomcat ... 24
5.2.4.4 4.4 Installation of JDK ... 24
5.2.4.5 4.5 Installation of SQL driver ... 25
5.2.4.6 4.6 Installation of Active Vos ... 25
5.2.4.7 4.7 Installation of BPM ... 25
5.2.5 5. Installation of Product 360 Media Manager ... 25
5.2.5.1 5.1 Installation of the database ... 25
5.2.5.2 5.2 Installation of the Media Manager ... 26
6 Database Installation ... 26
6.1 Pre-Installation Checklist ... 26
6.1.1 Database Administration Tool ... 26
6.1.2 Database Information ... 26
6.1.3 Default Product 360 Database Ports ... 26
6.2 DBMS Installation and Configuration Hints ... 27
6.2.1 Microsoft SQL Server ... 27
6.2.1.1 Server Settings ... 27
6.2.1.2 Named-Instance Support ... 31
6.2.2 Oracle ... 32
6.2.2.1 Server Settings ... 32
6.2.2.2 Database User Settings ... 35
6.2.2.3 DBA Tasks ... 35
6.3 Server Database ... 35
6.3.1 Custom Indexes ... 36
6.3.2 Oracle RAC, Oracle ASM (Automated Storage Management) ... 36
6.3.3 Minimum Oracle privileges ... 40
6.3.3.1 Normal installation (tablespaces and db users are not existing before install process) ... 40
6.3.3.2 Installation with restricted privileges (similar update) ... 42
6.3.4 Binaries ... 43
6.3.4.1 Extract the database setup archive ... 43
6.3.4.2 Provide database connection settings ... 43
6.3.4.3 Creating/Updating schemas - Microsoft SQL Server (GUI) ... 51
6.3.4.4 Creating/Updating schemas - Oracle (GUI) ... 53

6.3.4.5 Creating/Updating schemas (Headless) ... 55
6.3.5 Troubleshooting ... 55
6.4 Media Manager Database ... 55
6.4.1 Installing the Media Manager database ... 56
6.4.2 Oracle specific information ... 58
6.4.2.1 Create tablespaces manually for Oracle RAC, Oracle ASM (Automated Storage Management) ... 58
6.4.2.2 Minimum Oracle privileges ... 59
6.4.3 Microsoft SQL Server specific information ... 61
6.4.3.1 Operating the application without db_owner role ... 62
6.4.3.2 Operating the application without database user "OPASPUBLIC" ... 63
6.4.3.3 Installing full-text search for Microsoft SQL Server ... 64
6.4.3.4 Activating further iFilters on Microsoft SQL Server 2008 ... 65
6.4.4 Post-flight steps ... 66
6.5 Supplier Portal Database ... 66
6.5.1 Download the Product 360 Supplier Portal install file ... 66
6.5.2 Create your Database Installation Root ... 67
6.5.3 Setup initial database by install script ... 67
6.5.3.1 Configure the database properties in the configuration.properties file ... 67
6.5.3.2 Execute Setup.cmd script ... 71
6.5.4 Alternatively: Setup custom database manually ... 73
6.5.4.1 Setup Oracle Schema ... 73
6.5.4.2 Setup MS SQL Schema ... 75
7 Elasticsearch Installation ... 77
7.1 Prerequisites for the following products ... 77
7.2 Installing the Elasticsearch 7.x.x ... 77
7.3 Default Elasticsearch Ports ... 78
7.4 Installing the Kibana (optional) ... 78
7.5 Pre-Installation Checklist ... 78
7.5.1 Version Requirement ... 79
7.5.2 License Requirement ... 79
7.5.3 System Requirements ... 79
7.5.3.1 Memory Requirement ... 79
7.5.3.2 Hardware Requirement ... 79
7.5.4 Security Requirement ... 80

7.5.5 Further Reading ... 80
8 Server Installation ... 80
8.1 Prerequisite ... 81
8.1.1 OS User Permissions ... 81
8.1.1.1 Windows ... 81
8.1.1.2 Linux ... 83
8.1.2 OS Volume Shares and Permissions ... 84
8.1.2.1 Single Server ... 84
8.1.2.2 Multi Server ... 84
8.1.3 Default Product 360 Server Ports ... 84
8.1.4 Encryption of secure information ... 85
8.1.4.1 Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information ... 86
8.1.5 Large memory pages under Linux ... 86
8.2 Application Server ... 86
8.2.1 Download and Extract Binaries ... 87
8.2.2 Configuration ... 87
8.2.2.1 General Server Settings (server.properties) ... 88
8.2.2.2 Startup parameters (_environment.conf) ... 89
8.2.2.3 NetworkConfig ... 90
8.2.3 License ... 92
8.2.4 Service Installation ... 93
8.2.4.1 Windows ... 93
8.2.4.2 Linux ... 94
8.3 Media Asset Provider ... 94
8.3.1 Media Manager Provider ... 94
8.3.2 Classic Provider ... 94
8.3.2.1 GraphicsMagick for Classic Provider ... 94
9 Desktop Client Installation ... 95
9.1 Prerequisite ... 96
9.2 Binaries ... 96
9.3 Installing the client with MSI file ... 96
9.4 Starting the client ... 99
9.5 Single Sign-On ... 101
9.5.1 LDAP Authentication ... 101

9.5.2 SAML Authentication 102
10 Message Queue Installation 102
10.1 Prerequisites for the following products 102
10.2 Installing the Apache Message Queue 5.x.x 102
10.3 Run Apache Message Queue 5.x.x as a service 103
10.4 Enable the JMX for Apache Message Queue 103
10.5 Security (optional) 104
10.5.1 Use SSL over TCP 105
10.6 Clustering (optional) 105
11 Media Manager Installation 107
11.1 Prerequisite 107
11.2 Pre-Installation Checklist 107
11.2.1 OS User Permissions 107
11.2.1.1 Windows 107
11.2.2 OS Volume Shares and Permissions 107
11.2.3 Default Product 360 - Media Manager Ports 108
11.2.3.1 Port range 109
11.3 Media Manager Installation 110
11.3.1 Installation checklist 110
11.3.1.1 New installation 110
11.3.1.2 Update 110
11.3.2 Installing File Server 111
11.3.3 Installing Funcd 111
11.3.3.1 General information 112
11.3.3.2 File server Funcd 112
11.3.3.3 Second Pipeline Funcd (optional) 120
11.3.4 Installing the client modules 120
11.3.4.1 Installing the client modules 121
11.3.4.2 Installing and setting up the ODBC connection under Macintosh 122
11.3.5 Installing the web front end 123
11.3.5.1 Windows 123
11.3.5.2 Linux 125
11.3.5.3 Encrypted passwords in configuration files 129

11.3.6 Setting up PIM - Media Manager ... 129
11.4 Media Manager Integration ... 129
11.4.1 Product 360 - Server ... 130
11.4.1.1 Integrating Product 360 - Media Manager ... 130
11.4.2 Product 360 - Desktop Client ... 143
12 Supplier Portal Installation ... 143
12.1 Pre-Installation Checklist ... 143
12.1.1 OS User Permissions ... 143
12.1.1.1 Windows ... 143
12.1.1.2 Linux ... 143
12.1.2 Product 360 - Supplier Portal Default Ports ... 144
12.1.2.1 Change Application Server Ports ... 144
12.2 Supplier Portal Integration ... 145
12.2.1 Prerequisite ... 146
12.2.2 Software Upgrade(10.5.02.01 onwards) ... 146
12.2.3 Setup Product 360 Core Users and Permissions till 10.5.0.02 ... 146
12.2.3.1 Create required Users and Groups within Product 360 - Desktop ... 147
12.2.3.2 Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/Viewer ... 157
12.2.4 Setup Product 360 Core Users and Permissions starting from 10.5.02.01 ... 157
12.2.4.1 Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/Viewer ... 158
12.2.4.2 Create required Users and Groups within Product 360 - Desktop ... 159
12.2.5 Setup communication Product 360 Server - Product 360 Supplier Portal ... 170
12.3 Media Manager and Supplier Portal Integration ... 172
12.3.1 Prerequisite ... 172
12.3.2 Setup Hotfolder ... 172
12.3.3 Setup REST Service ... 176
12.3.3.1 Tomcat and Java ... 176
12.3.3.2 Installation HMM REST war ... 176
12.3.3.3 Configuration HMM REST war ... 176
12.3.3.4 Startup ... 177
12.4 Web and Supplier Portal Integration ... 178
12.4.1 Prerequisite ... 178
12.4.2 Configure Product 360 Supplier Portal Item Editor System User within Product 360 - Web ... 178
12.5 Server Installation on Windows ... 179

12.5.1 Prerequisite ... 179
12.5.2 Download the Product 360 Supplier Portal zip ... 179
12.5.3 Create Your Product 360 Supplier Portal Server Installation Root ... 180
12.5.4 Configuration ... 180
12.5.4.1 Configure Product 360 Supplier Portal central configuration file ... 180
12.5.4.2 Configure Logging ... 185
12.5.5 Install Tomcat ... 185
12.5.5.1 Install Product 360 - Supplier Portal Tomcat Windows Service ... 185
12.5.5.2 Start/Stop/Configure Product 360 - Supplier Portal Tomcat Windows Service ... 186
12.5.5.3 (optional) Uninstall Product 360 - Supplier Portal Tomcat Windows Service ... 187
12.6 Server Installation on Linux ... 187
12.6.1 Prerequisite ... 187
12.6.1.1 Java ... 187
12.6.2 Download the Product 360 Supplier Portal zip ... 188
12.6.3 Create Your Product 360 Supplier Portal Server Installation Root ... 188
12.6.4 Configuration ... 188
12.6.4.1 Configure Product 360 Supplier Portal central configuration file ... 188
12.6.4.2 Configure Logging ... 192
12.6.5 Install Tomcat ... 193
12.6.5.1 Install Product 360 - Supplier Portal Tomcat Linux Service ... 193
12.6.5.2 Start/Stop Supplier Portal Tomcat Server ... 194
12.6.5.3 Deinstallation ... 194
12.7 Language Pack Installation ... 195
12.7.1 Overview ... 195
12.7.2 Installation ... 195
12.8 Installation Troubleshooting ... 195
13 Business Process Management ... 198
13.1 Informatica BPM Installation ... 199
13.1.1 Informatica BPM Installation ... 199
13.1.1.1 Installation of the Informatica BPM service ... 199
13.1.1.2 Webserver and Java ... 200
13.1.1.3 Integrated Security ... 201
13.1.2 Installation of the required default workflows ... 202
13.1.3 Configure Dispatch Services ... 205

13.1.4 Preparing Informatica BPM service for JMS based communication 208
13.1.4.1 Download additional library 208
13.1.4.2 Setup messaging service within Informatica BPM 208
13.2 BPM specific configuration within server.properties 212
13.2.1 Message queue communication properties 213
13.2.2 General properties 215
13.2.3 REST communication properties 216
13.2.3.1 Simple connectivity test 218
13.2.3.2 Service endpoints and partner links within Informatica BPM workflows 219
13.3 Failsafe handling of calls to Informatica BPM 220
13.4 Message Queue Based Communication 222
13.5 Delayed message delivery 222
13.5.1 Objective 222
13.5.2 General 222
13.5.3 Configuration 223
13.5.3.1 Configuration of Active MQ server 223
13.5.3.2 Product 360 configuration (server.properties) 224
14 Web Search Installation 224
14.1 Pre-Installation Checklist 224
14.1.1 Version Requirement 225
14.1.2 License Requirement 225
14.1.3 System Requirements 225
14.1.3.1 Memory Requirement 225
14.1.3.2 Hardware Requirement 225
14.1.4 Security Requirement 226
14.1.5 Further Reading 226
14.1.6 Elasticsearch Installation on Windows 226
14.2 Web Search Integration 226
14.2.1 Prerequisite 226
14.2.2 Setup Product 360 Permissions for Web Search 226
14.2.2.1 Permission Settings for Product 360 - Web User to use Web Search 227
14.2.2.2 Permission Settings for Product 360 - Desktop User to use Web Search Index Build 227
14.2.3 Setup Configuration for Product 360 - Repository 227
14.2.4 Setup Configuration for Product 360 - Core 228

14.2.5 Setup Configuration for Product 360 - Desktop 229
14.2.6 Setup Configuration for Product 360 - Web 230
14.3 Installation Troubleshooting 230

Informatica MDM - Product 360 is a client server application with multiple optional modules. In general, all modules can be installed on the same host. For performance and load balancing reasons we recommend to use multiple host machines. This deployment guide gives an overview on the possible deployment scenarios and provides detailed installation instructions for each of the modules.

Please refer to the Sizing Guide to get an overview on the needed hardware for your individual project.

- Pre-Installation Checklist (see page 11)
- Logical Service Overview (see page 11)
- General Communication Overview (see page 12)
- Port Overview (see page 13)
  - Database (see page 13)
  - Server, Web and Desktop (see page 14)
  - Elasticsearch (see page 15)
  - Media Manager (see page 15)
  - Port range (see page 16)
    - Supplier Portal (see page 17)

1 Pre-Installation Checklist

Before beginning to install, please check that:

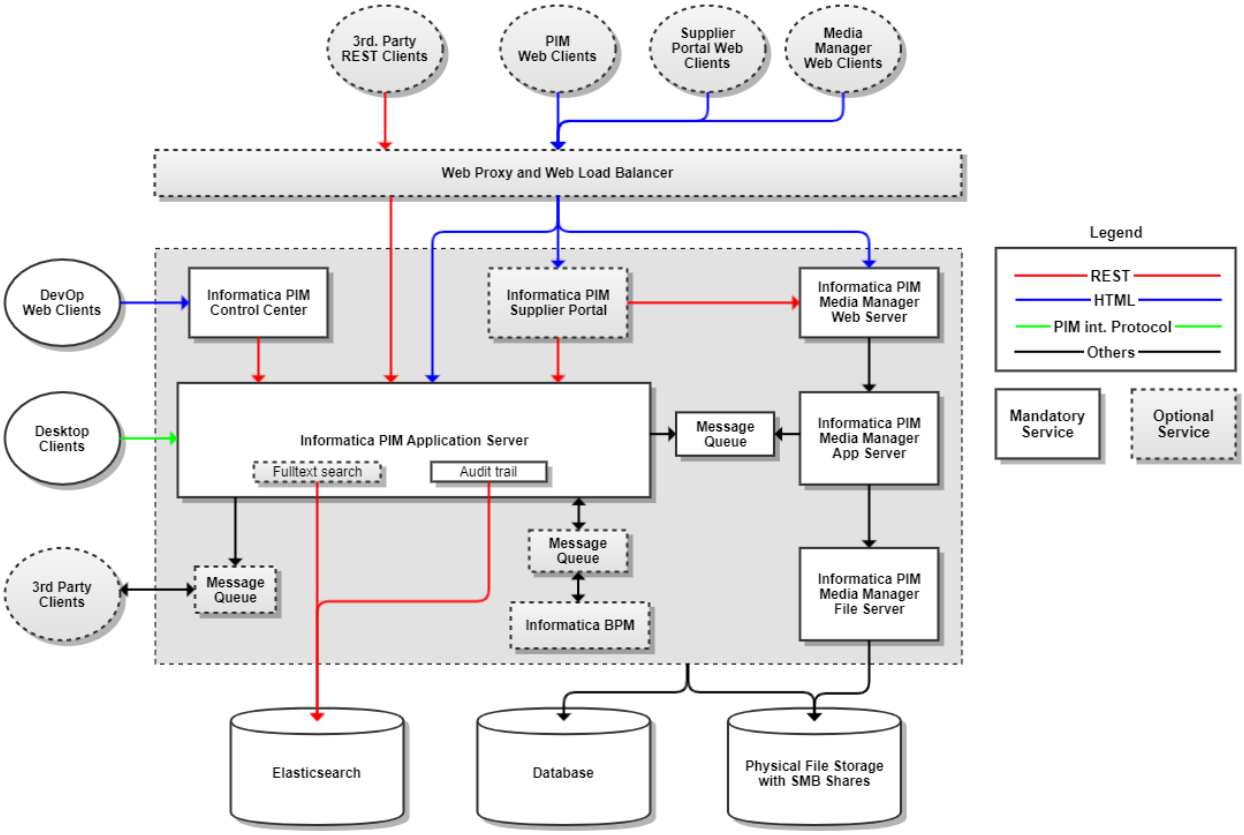
- Your system meets the requirements of the Product Availability Matrix (PAM)

  ⚠ Note: Please find the Product Availability Matrix in Informatica Network

- You must be able to use a command prompt to continue. If not, please contact your system administrator to assist.
- If you have not downloaded the binary packages already, please raise a Shipping Request with Informatica.

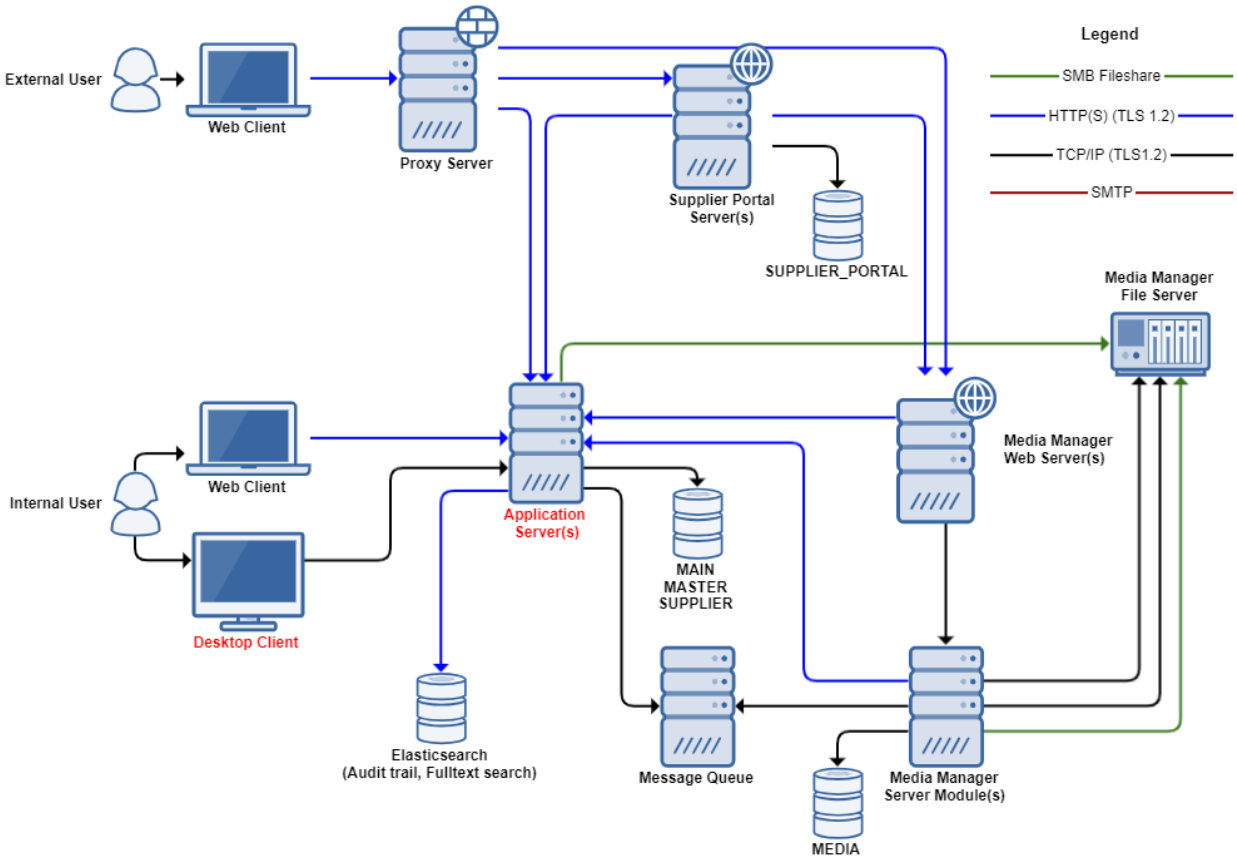
2 Logical Service Overview

The following diagram gives a logical overview on the services which are involved in the overall Product 360 application. The deployment strategy should be individually defined based on the sizing requirements of the customer. Examples for a typical and full deployment can be found alter in this chapter.



3 General Communication Overview

The diagram shows the general communication connections between the modules of the installation. Mandatory modules are marked in red. The complete list of all communication ports can be found below the diagram. This overview shows only a single server and it omits also load balancing servers/ modules since they are identical or common technology.



4 Port Overview

4.1 Database

Port	Database
1433	MSSQL
1521	Oracle

4.2 Server, Web and Desktop

Port	Protocol	Product 360 Module
1712	tcp/tcps	Desktop connection. This port is used to connect the Desktop Client with it's Server as well as each server with each other server. The used protocol is an internal low-level protocol, optimized for high performance throughput. TLS 1.2 can be used for this protocol.
1512	http/https	Web Server Port (Jetty) which is used for the Web Client as well as the Service API or file transfer. The used protocol is HTTP or HTTPS (or REST via HTTP). TLS 1.2 is supported.
1812	tcp	Data Grid communication. Needed for the synchronization heartbeat of the cluster. No data is transferred with this protocol, only synchronisation tokens.
55555	tcp	Default Java Management Extensions Port which is needed to attach troubleshooting and tuning tools. For security reasons this port must not be reachable from outside the server machine.
61616	tcp/tcps	The port for the message queue connection.
25	smtp	Product 360 - Server is capable to send e-mails in various functional areas, for this it needs access to an smtp e-mail server
445 and 139	smb and tcp	Windows file share ports for the media asset file communication when used with the Product 360 - Media Manager module

4.3 Elasticsearch

Port	Protocol	Product 360 Module	Description
9200	http/https	Audit trail and Fulltext search	This port is used by Product 360 - Server to communicate with Elasticsearch for Audit trail and Fulltext search

4.4 Media Manager

Port	Protocol	Product 360 Module
11100	tcp	Funcd
11101	tcp	Pipe Funcd
11102	tcp	Internet Funcd
81	tcp	Product 360 Core and Product 360 - Media Manager Web - XOB Connection
8089	http	Session Manager, Web Status Page
8080	http	Product 360 - Media Manager Web, Product 360 - Media Manager REST
82	tcp	Product 360 - Media Manager Web XOB Connection (Administration) (optional for Product 360 8 only for upgrade)
83	tcp	Product 360 - Media Manager Web XOB Connection (Data) (optional for Product 360 8 only for upgrade)

Port	Protocol	Product 360 Module
84	tcp	Product 360 - Media Manager Web XOB Connection (Data) (optional for Product 360 8 only for upgrade)
8161	tcp	MessageQueue
61616	tcp	MessageQueue
8009	tcp	Product 360 - Media Manager Web, ajp13/mod_jk connector
59170 - 60678	tcp	Product 360 - Media Manager desktop modules (Workflowmanager) (see port range calculation below)
445 ,139	smb, tcp	Windows file share ports for the Product 360 Core and Product 360 - Media Manager file communication

4.5 Port range

Formula to calculate the port number of a module: **Portnumber = modulo(StationId,100) * 15 + 59169 + ModuleId**

==> New possible port range: 59170 - 60678

Module	Module Id	Port for Station 100	Port for Station 199
Process Watcher	1	59170	60655
Pipeline	2	59171	60656
Xob Adminconsole	3	59172	60657

Module	Module Id	Port for Station 100	Port for Station 199
Mediapublisher	4	59173	60658
Workflowmanager	5	59174	60659
XML Connector	6	59175	60670
Hotfolder	7	59176	60671
Archive	8	59177	60672
Interface	9	59178	60673
Medias	11	59180	60675
Production	12	59181	60676
Administration	14	59183	60678

4.5.1 Supplier Portal

Port	Protocol	Product 360 Module
9090	http	Product 360 - Supplier Portal (Tomcat Application Server)
25	smtp	Mail Server
8080	http	Product 360 - Media Manager REST

Port	Protocol	Product 360 Module
1512	http	Product 360 - Server Service API

5 Step by Step installation guide

The purpose of this document is to have a step by step guide for the installation of all Product 360 modules. It defines the installation order of the different modules as well as some pre-requisites.

5.1 Pre-Requisites

The Product 360 application family provides all necessary software which is needed to run the applications except an operating system and a database server.

5.1.1 Pre-Requisites for Product 360 Supplier Portal

The setup script requires a database command-line tool in the windows PATH environment variable:

- in case of Oracle this is sqlplus
- while MS SQL Server uses sqlcmd

5.1.2 Pre-Requisites for Active Vos

Active Vos has special Pre-Requisites which are not provided by Informatica. The Pre-Requisites are:

- A Tomcat Application Server 7.x or 8.x
- A JDK 1.7 or 1.8
- JDBC driver (Version depends on your database)

Please also check the Active Vos PAM for other versions or updates.

5.1.3 Documentation

The provided download folder at our download portal network.informatica.com contains the file "PIM_<version>_Installation_and_Operation.zip". This archive contains all necessary installation and operation manuals for all products except for ActiveVos which is available at the internet. This installation checklist refers to specific chapters within these manuals, so it is highly recommended to extract this archive to a location of your choice. The zip should contain the following manuals:

Manual	Needed by this guide
PIM_<version>_ConfigurationManual.pdf	✓
PIM_<version>_Installation_and_Operation.pdf	✓
PIM_<version>_InstallationManual.pdf	✓
PIM_<version>_MigrationManual.pdf	✗
PIM_<version>_OperationManuel.pdf	✗
PIM_<version>_SizingManual.pdf	✗
ActiveVos Installation Manual (http://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp)	✓

5.1.4 Operating system

We assume that an Operating system is already installed. We provide a Product Availability Matrix which is available in the chapter *Product Availability Matrix (PAM)* of the *Installation and Operation Manual* and lists all supported operating systems.

5.1.4.1 Data Quality

> Starting with version 10.1.0.02 the IDQ SDK and engine have been upgraded to version 10.5.
> This requires some actions to ensure that server is starting properly and Data Quality features can be used further.

Only if Microsoft Server is used: download and install MSVC Redistributable from official Microsoft site.

Visual Studio 2015, 2017 and 2019

Download the Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. The following updates are the latest supported Visual C++ redistributable packages for Visual Studio 2015, 2017 and 2019. Included is a baseline version of the Universal C Runtime see MSDN for details.

- x86: vc_redist.x86.exe
- x64: vc_redist.x64.exe
- ARM64: vc_redist.arm64.exe

Note Visual C++ 2015, 2017 and 2019 all share the same redistributable files.

5.1.5 Application and install file matrix

This matrix shows which file(s) are needed to install the corresponding application. As mentioned before these file(s) can be downloaded at the informatica download portal network.informatica.com under "Resources".

Application	File(s)	Mandatory
Product 360 Server Product 360 Rich/Web Client	PIM_<version>_Core.zip	✓
Product 360 Accelerators	PIM_<version>_Accelerators.zip	✗
Product 360 Supplier Portal	PIM_<version>_SupplierPortal.zip, PIM_<version>_SupplierPortal_Languages.zip	✗
Active Message Queue	PIM_<Version>_ThirdPartySoftware.zip	✓
ActiveVos	ActiveVOS_Server_windows_9.2.4.exe	✓

Application	File(s)	Mandatory
Product 360 Media Manager	PIM_<version>_MediaManager.zip, PIM_<version>_MediaManager_Languages.zip, PIM_<version>_ThirdPartySoftware.zip	✗

5.2 Installation of Product 360 applications

This is a step by step list of an installation of all applications of the Product 360 family. Except the Product 360 server all applications are optional and so must only be installed if needed. It´s highly recommended to follow this installation order, if any application is not needed it can simply be skipped. It is also recommended to see the Prerequisite chapters of the installation manuals.

5.2.1 1. Installation of the Product 360 Server

Required installation file(s)	Required documentation	Required installations	Mandatory
• PIM_<version>_Core.zip	• PIM_<version>_InstallationManual.pdf • PIM_<version>_Installation_and_Operation.pdf • PIM_<version>_ConfigurationManual.pdf (optional)	---	✓

5.2.1.1 1.1 Installation of the database

The first step of the installation is to install the database for Product 360 server. The supported database servers are mentioned in the chapter *8.4 Database Server* of the *Installation and Operation* manual.

A detailed installation manual can be found in chapter *6 Database Installation* of the *Installation manual.* In case that the database is already installed, this step can be skipped of course.

5.2.1.2 1.2 Installation of the Product 360 Control Center

After installing the database the Control Center has to be installed. The Control Center is the central application for installation and operation of the Product 360 server cluster. It must also be used for single server installations.

To install the Control Center please follow the steps of chapter *7.1 - 7.2.2* of the *Installation Manual*. Chapter 7.2.2 can be skipped in case of a single server installation.

5.2.1.3 1.3 Installation of Active Message Queue

Required installation file(s)	Required documentation	Required installations	Mandatory
• PIM_<Version>_ThirdPartySoftware.zip	• PIM_<version>_InstallationManual.pdf	---	• for Product 360 Server • for Product 360 Media Manager

The installation of the Active Message Queue has to be done before installing the Product 360 application server. The installation of the Message Queue is described in detail in chapter *9.1 -9.6 Message Queue Installation* of the *Installation Manual*.

5.2.1.4 1.4 Installation of Elasticsearch

The Elasticsearch server can be downloaded from the internet. It is recommended to install Elasticsearch server on dedicated hardware.

The installation of the Elasticsearch server has to be done before installing the Product 360 application server. The installation of the Elasticsearch server is described in detail in chapter *Elasticsearch Installation* of the *Installation Manual*.

> Elasticsearch server is mandatory for a Product 360 production installation.

5.2.1.5 1.5 Installation of the Product 360 Application server

Finished the Control Center installation the Product 360 application server can be installed. This installation is described in chapter *7.3.1 - 7.3.4 Application Server* of the *Installation Manual*, additional configuration details can be found in the *Configuration Manual* chapter *4 Server Configuration*.

For the monitoring described in chapter *7.3.4 Enable Monitoring in Control Center* of the *Installation Manual* the desktop client has to be installed. This will be done in the next step.

5.2.2 2. Installation of the Product 360 Desktop Client

Required installation file(s)	Required documentation	Required installations	Mandatory
• PIM_<version>_Core.zip	• PIM_<version>_InstallationManual.pdf	• Product 360 Server	✔

To verify if the Product 360 server installation was successful and for later configurations the Desktop Client can be installed now. The installation is described in detail at chapter *8.1 - 8.4 Desktop Client Installation* of the *Installation Manual*. Single Sign-On options can be found in chapter *8.5.1 and 8.5.2*.

5.2.3 3. Installation of the Product 360 Supplier Portal

Required installation file(s)	Required documentation	Required installations	Mandatory
• PIM_<version>_SupplierPortal.zip • PIM_<version>_SupplierPortal_Languages.zip (optional)	• PIM_<version>_InstallationManual.pdf	• Product 360 Server • sqlplus or sqlcmd	✘

5.2.3.1 3.1 Installation of the database

The Supplier Portal has its own database which has to be installed in this step. It is only required if the Supplier Portal will be installed, otherwise it can be skipped. A detailed installation guide can be found in chapter *6.5 Supplier Portal Database* of the *Installation Manual*.

5.2.3.2 3.2. Installation of Supplier Portal

The next step is the installation of the Supplier Portal. The installation of the Supplier Portal is optional and can be skipped if this application is not needed. A detailed installation manual can be found at chapter *11 Supplier Portal Installation* of the *Installation Manual*

5.2.4 4. Installation of BPM / ActiveVos

Required installation file(s)	Required documentation	Required installations	Mandatory
ActiveVOS_Server_windows_9.2.4.exe	• PIM_<version>_InstallationManual.pdf • http://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp?nav=%2F3_0	• Product 360 Server • A Tomcat Application Server 7.x or 8.x • A JDK 1.7 or 1.8 • JDBC driver	✕

The installation of ActiveVos is described in detail at http://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp. The ActiveVos installation file can also be downloaded from the informatica download portal network.informatica.com.

5.2.4.1 4.1 Installation of the database

Create a database and a database user (this step can be skipped if the database already exists)

- The name can be chosen freely, we recommend to user the default "ActiveVOS"
- The user can also be chosen freely, but we recommend the default "bpeluser"

More details can be found in the documentation at chapter Server Installation, Configuration, and Deployment > Apache Tomcat >Configuration.

5.2.4.2 4.2 Create a Active Vos root folder

After creating the database an Active Vos root folder should be created. It can be created parallel to the Product 360 root folder for example and will be called <ActiveVosRoot> in this documentation.

5.2.4.3 4.3 Installation of Tomcat

The Tomcat Application Server can be downloaded in the internet. It is recommended to create a Tomcat folder within the <ActiveVosRoot> folder and unzip the Tomcat application server to this directory.

5.2.4.4 4.4 Installation of JDK

Create a JDK folder within the <ActiveVosRoot> folder. Afterwards the JDK must be installed to this directory. If you already have a JDK installed you can skip this step and later point to the existing JDK. The version should be supported of course.

5.2.4.5 4.5 Installation of SQL driver

As a next step create a folder within the <ActiveVosRoot> folder, download the corresponding jdbc driver and copy or unzip it to the created folder.

5.2.4.6 4.6 Installation of Active Vos

Run ActiveVOS_Server_windows_9.2.4.exe and follow the installation wizard. The installtion directory can be chosen freely and is needed in the next step.

After the installation was completed successfully, navigate to <installationDirectory>/Server/server-enterprise/tomcat_config/bin> and execute the config_deply.bat as administrator. Follow the Install wizard and note that there is a "help" button at the lower left corner which can give you some useful help.

On the Database Configuration page the username and password is required which was defined in step 6.1 as well as the jdbc driver jar file which was installed in step 6.4.On the Application server path wizard page, the folder which was created in step 6.2 is required.

As a last step the Tomcat Application server must be started. The start file can be found within the bin folder of the Tomcat directory, which has been created in step 6.2.

To verify if the installation was successful open http://<hostname>:<port>/active-bpel/ .

5.2.4.7 4.7 Installation of BPM

After installing ActiveVos BPM can be installed and configured. A detailed installation guideline can be found at chapter *13.2 Business Process Management* in the *Installation Manual*.

5.2.5 5. Installation of Product 360 Media Manager

Required installation file(s)	Required documentation	Required installations	Mandatory
• PIM_<version>_MediaManager.zip • PIM_<version>_MediaManager_Languages.zip • PIM_<version>_ThirdPartySoftware.zip	• PIM_<version>_InstallationManual.pdf	• Product 360 Server	✕

5.2.5.1 5.1 Installation of the database

The first step of the installation of the Product 360 Media Manager is the installation of the database. A detailed guide is provided in the *Installation Manual* chapter *6.4 Media Manager Database*.

5.2.5.2 5.2 Installation of the Media Manager

The second step is the installation of the Product 360 Media Manager. This installation is described in the *Installation Manual* chapter *10 Media Manager Installation*.

6 Database Installation

6.1 Pre-Installation Checklist

During database installation you will going to :

- Create a new schema
- Create a user with full read/write access to the Product 360 schemas, including the ability to create tables

So you will need a database user which has enough permissions to create other users and schemas, talk to your local DBA to get you an appropriate account. To setup a database and the database user management is not the scope of this installation instruction, however you will find some database setup/configuration hints in the next section DBMS Installation and Configuration Hints (see page 27) which should support you with the important points in matter of the Product 360 database installation.

6.1.1 Database Administration Tool

- For database setup and configuration you will need a Database Administration Tool. For example MS SQL Server Management Studio or Oracle SQL Developer
- After the database setup Test the connection by using the database administration tool installed on the Product 360 server to log in to the database

6.1.2 Database Information

- During database setup you will have to provide a physical volume location on where to store the data and log files of the Product 360 databases
- In case you need to use the special character '\' for an instance name of your database, you have to escape it with an additional backslash.
  E.g. your instance name for a database is 'myDatabase\myInstance' then you have to define 'myDatabase\\myInstance' in the properties file

6.1.3 Default Product 360 Database Ports

- Ensure you be aware of the database ports your database server is running on.

Port	Database
1433	MSSQL
1521	Oracle

6.2 DBMS Installation and Configuration Hints

- Microsoft SQL Server (see page 27)
  - Server Settings (see page 27)
    - Maximum Degree of Parallelism (MAXDOP) (see page 27)
    - Number of TempDB Files (see page 28)
    - Server Collation (see page 28)
    - Database User Settings (see page 29)
      - Database setup user (see page 29)
  - Named-Instance Support (see page 31)
- Oracle (see page 32)
  - Server Settings (see page 32)
    - Degree of Parallelism (DOP) (see page 33)
    - Recommended initialization parameters (see page 33)
  - Database User Settings (see page 35)
  - DBA Tasks (see page 35)

Usually your DBA already installed the DBMS software for you and he is responsible to make sure that all load requirements
can be met by the configuration of the system. However, we wanted to share our experiences with the installation and especially
the configuration of the DBMS system so you experience the best performance possible.

6.2.1 Microsoft SQL Server

When installing MS SQL Server the following settings must be considered.

6.2.1.1 Server Settings

Maximum Degree of Parallelism (MAXDOP)

It is strongly recommended to set MAXDOP to 1 for all Product 360 Schemas/Databases since Product 360 is a high transaction multi-user OLTP application.

Number of TempDB Files

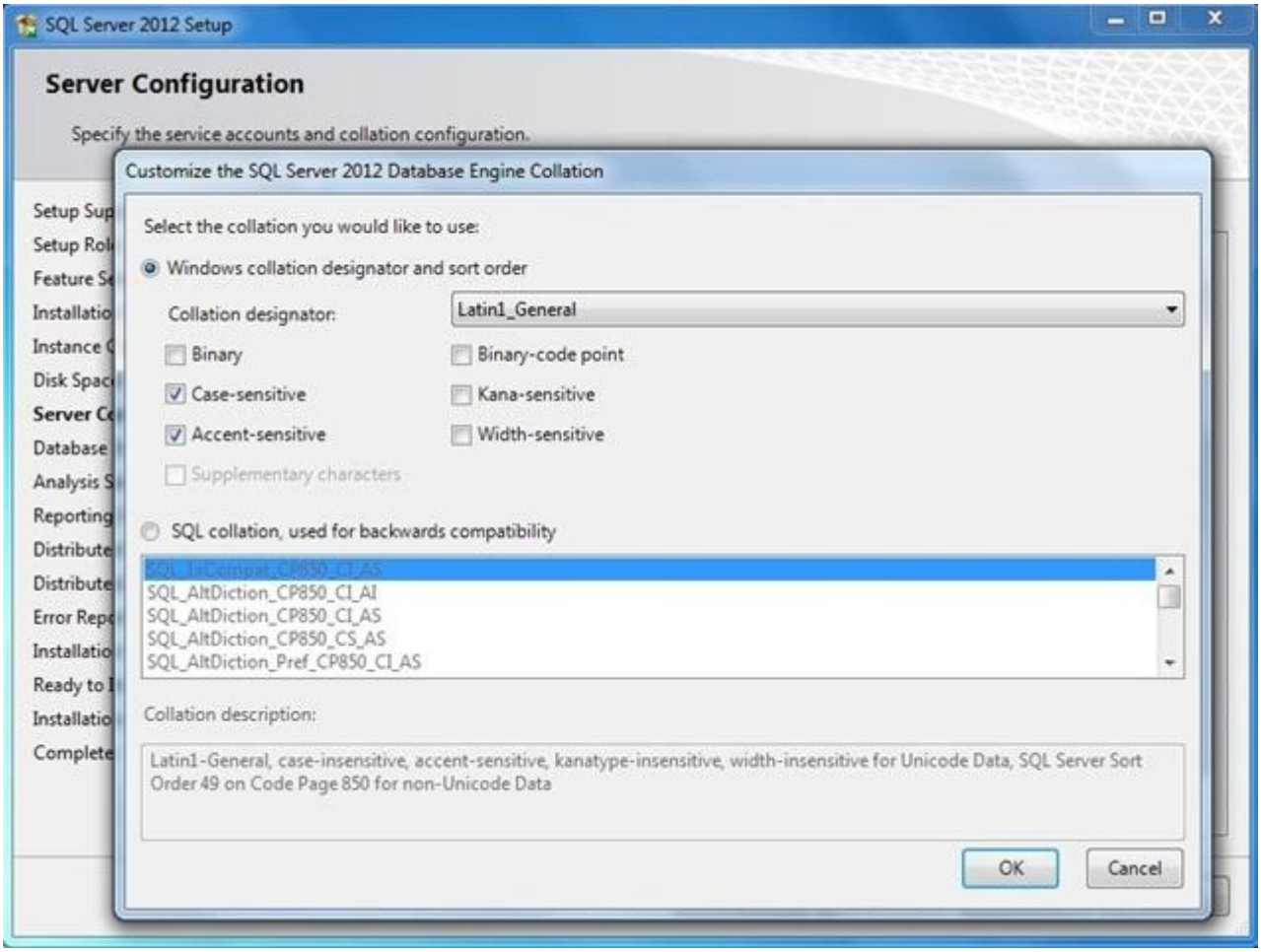
Since all Product 360 Schemas/Databases use the SNAPSHOT isolation mode of SQL Server a high temp DB throughput is required. We recommend to have a tempdb file for each physical CPU core (till up to 8 files).

See also the corresponding knowledge base article from Microsoft: https://technet.microsoft.com/en-us/library/ms175527(v=sql.105).aspx

Server Collation

While setup the Microsoft SQL Server for the "Server Collation" setting use ***Latin1_General*** and additional the options ***Case sensitive*** and ***Accent sensitive*** (`Latin1_General_CS_AS`).

Screenshot: Setup SQL Server 2012

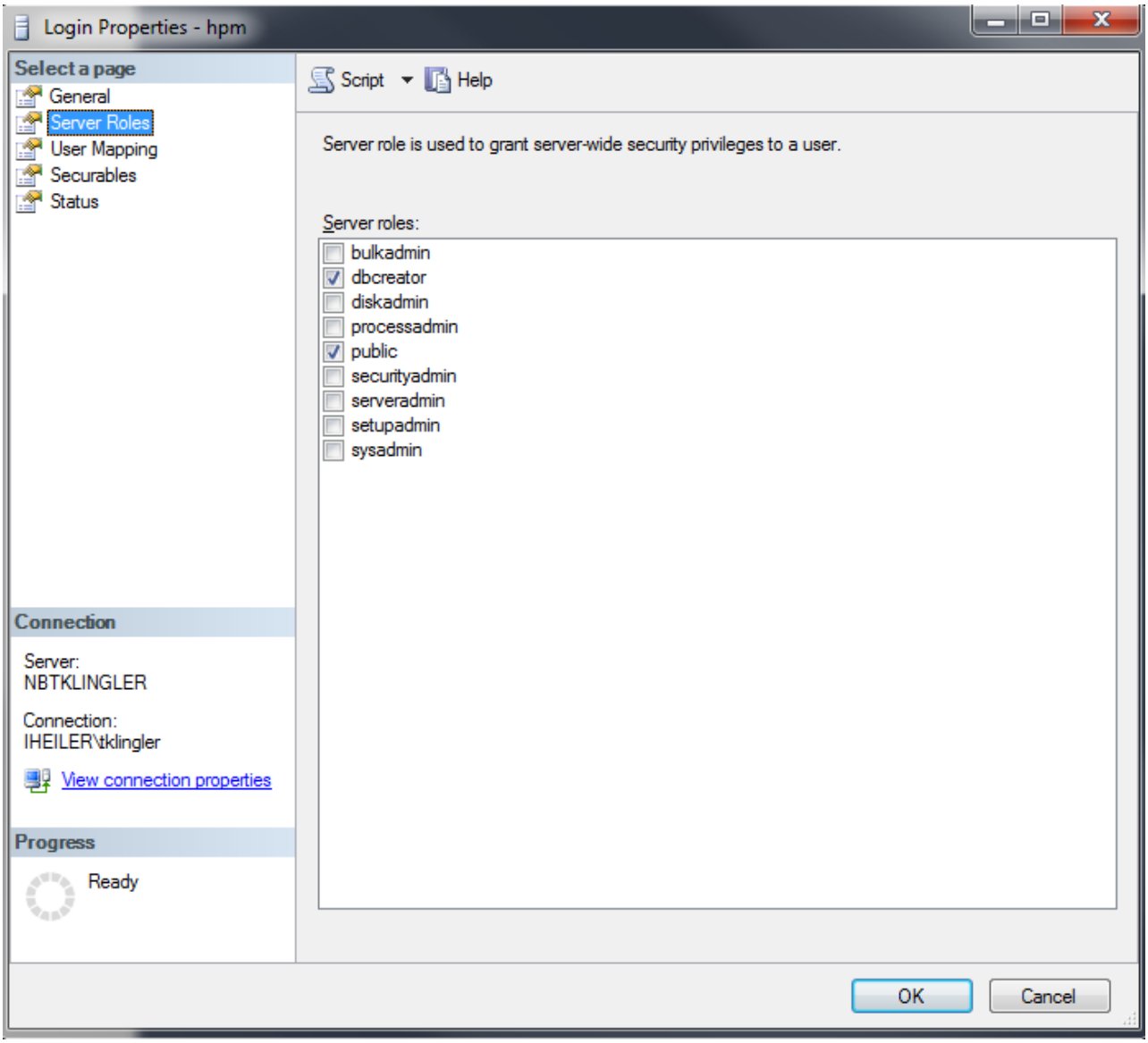


Database User Settings

Database setup user

The users which install the Product 360 schemas must have set the roles **DBCreator** and **Public**.

Screenshot: SQL Server Management Studio 2012 login properties dialog

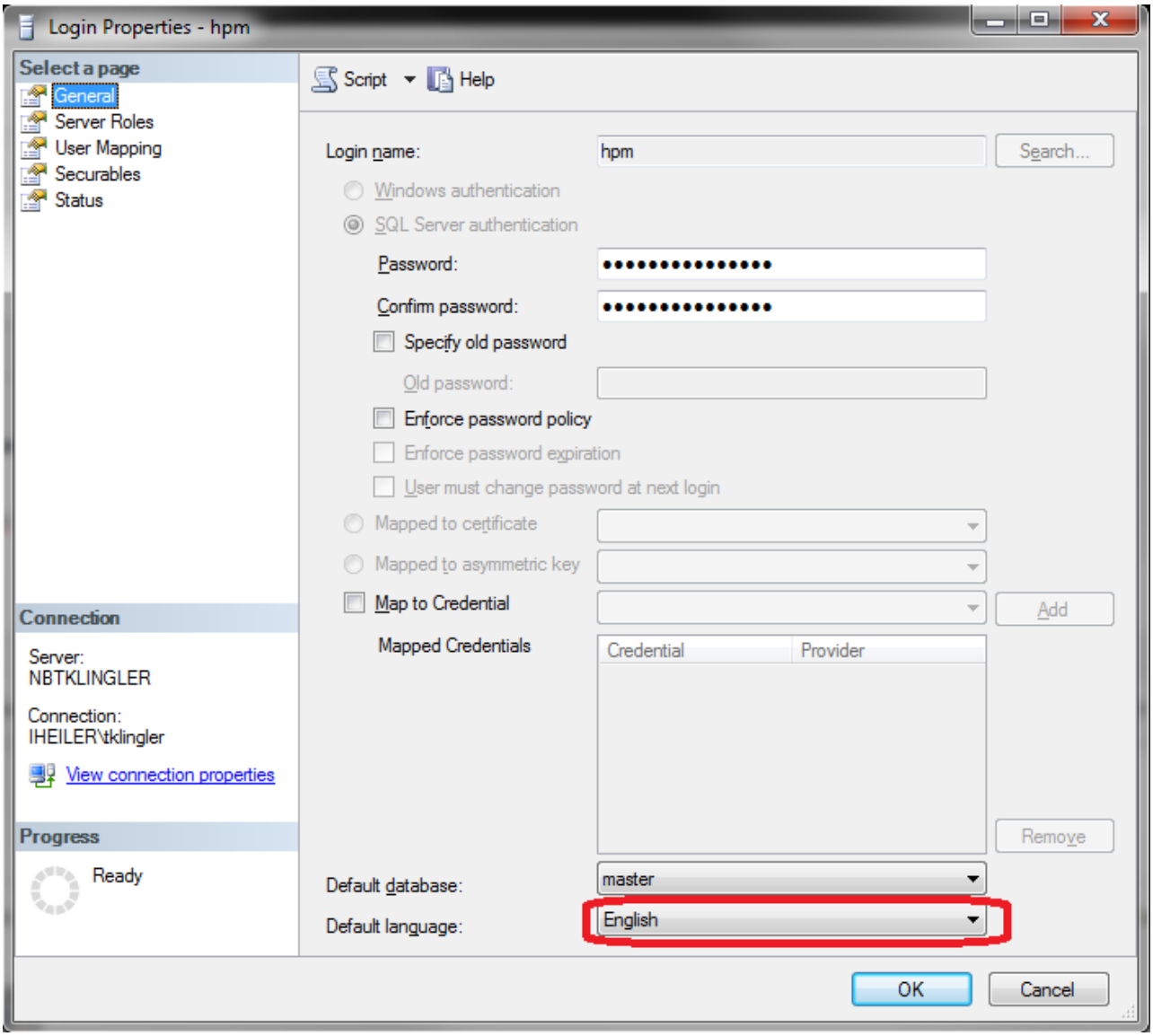


Database application users

All database users which are used for the database access of the Product 360 applications must always have **English** as standard language. Additionally uncheck the **Enforce password policy** checkbox.

Note: If integrated authentication should be used (see property "db.integrated.security" in server.properties file) "Windows authentication" has to be enabled for the database user.

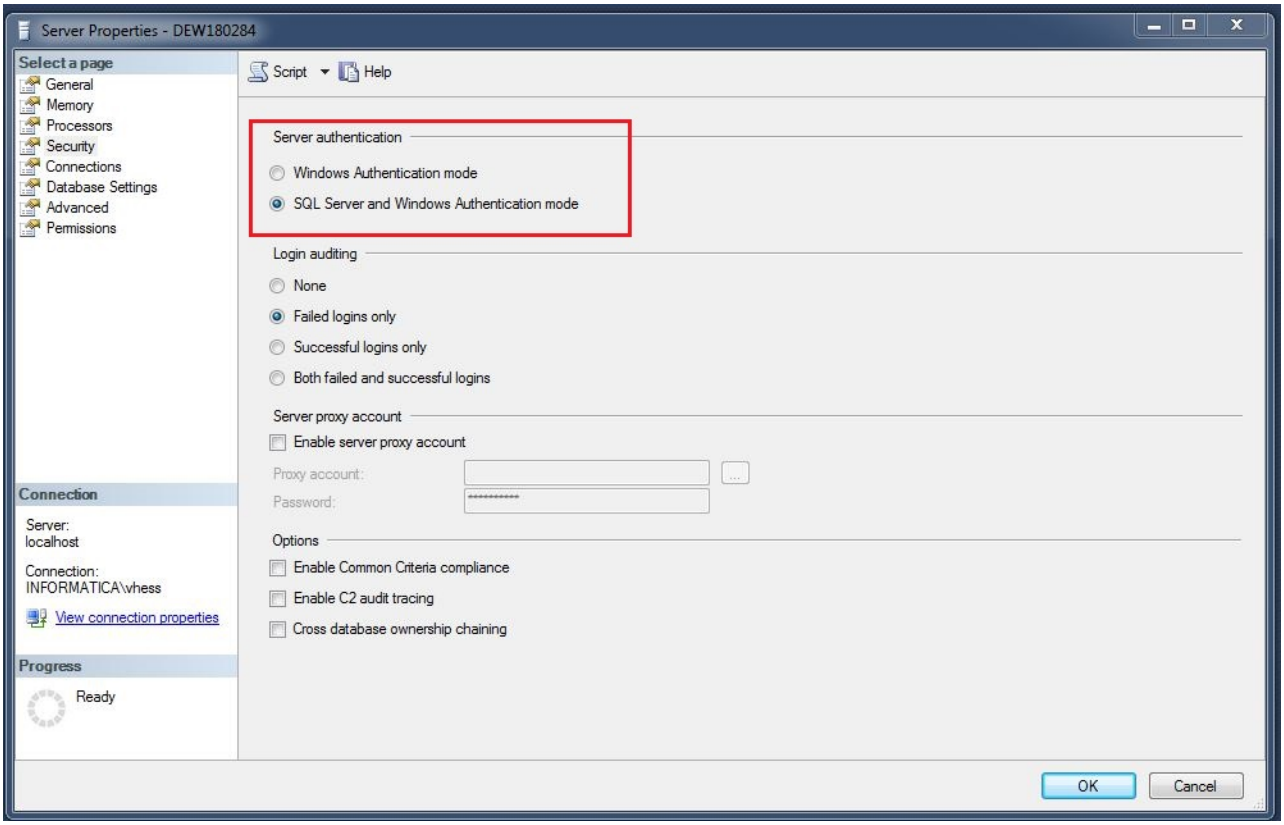
Screenshot: SQL Server Management Studio 2012 login properties dialog



Pay attention that the maximum size of memory of the SQL Server process is fixed. Otherwise the system may freeze possibly very fast. Also check the minimum size of memory and pay attention that the value is not greater than the available central memory. More Information

Authentication Mode

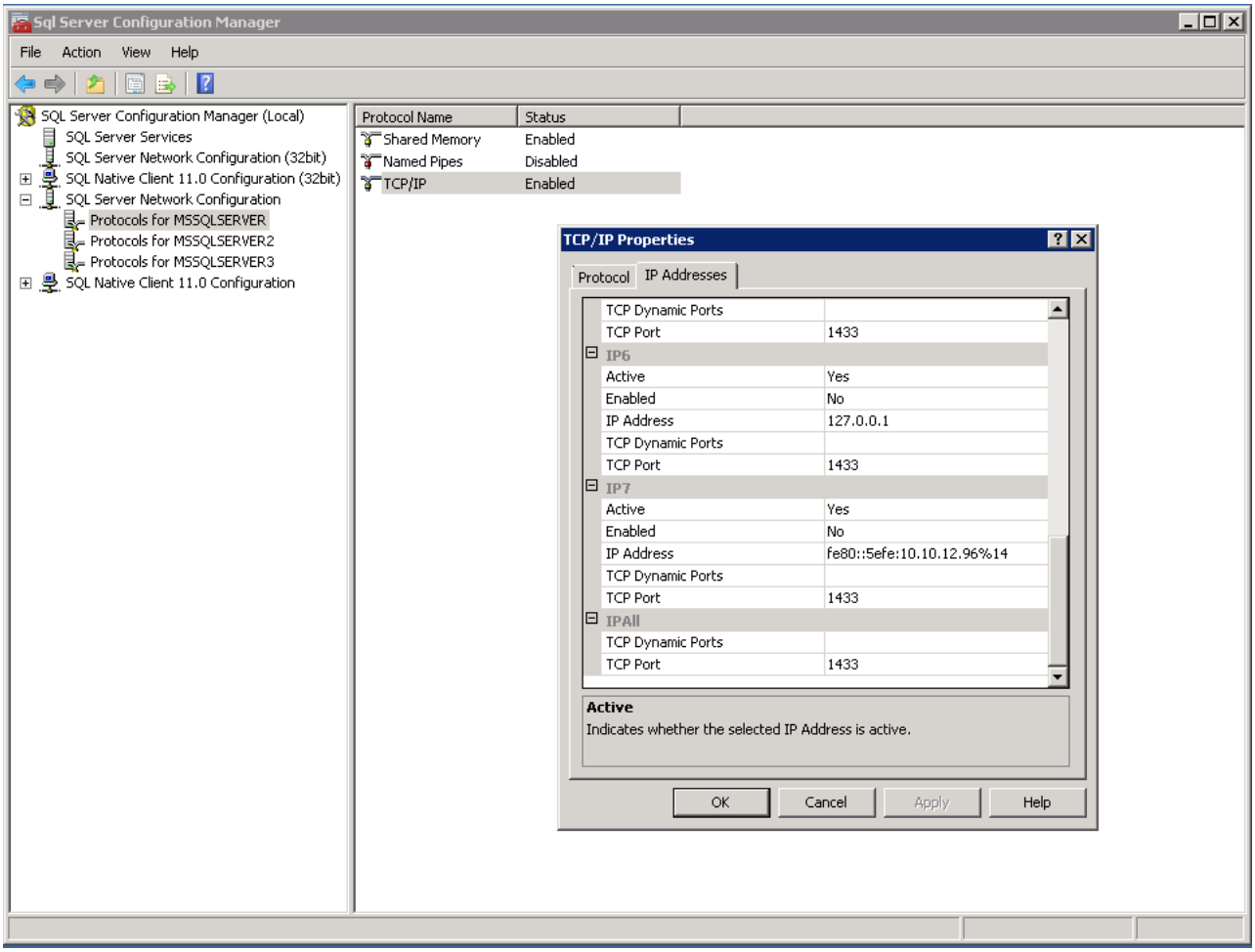
In order to authenticate to the database with the created SQL Server user, you have to check if the sever authentication mode accepts SQL Server users. Therefore connect to the management studio and right click on the top node and click on properties. Select security and check the server authentication mode.



6.2.1.2 Named-Instance Support

Informatica Product 360 can connect to MS-SQL Server named instances by using their port. Make sure that the **MS SQL Server Network Configuration** is correct. In section `IPAll` the `TCP Port` property must be set to a free port (Default is 1433), and `TCP Dynamic Ports` must be ***disabled*** as shown in the screenshot.

Screenshot: MS SQL Server Configuration Manager 2012, showing the properties of the TCP/IP Network configuration



1 Screenshot: MS SQL Server Configuration Manager 2012, showing the properties of the TCP/IP Network configuration

> Make sure that you restart the SQL service after that change.

6.2.2 Oracle

Consider these settings during installation of the database instance.

6.2.2.1 Server Settings

- Enable at least the feature "Enterprise Manager Repository"
- Set database character set to Unicode (`AL32UTF8`)
- Set the national specific character set to `AL16UTF16` - Unicode UTF-16 Universal character set

- Set standard increase redo-log file size to `1024 MB` (each), have at least three redo-logs
- Set standard language to American.
- Create a tnsnames.ora file at `<OracleDBInstanceFolder>/NETWORK/ADMIN` and map service names to the connect descriptors for the local naming method
- Disable password expíration, otherwise ensure that passwords for Product 360 schemas never expire
- Ensure have enough space for TEMP tablespace

Degree of Parallelism (DOP)

It is strongly recommended to set `PARALLEL_DEGREE_LIMIT` to 1 for all Product 360 Schemas/ Databases since Product 360 is a high transaction multi-user OLTP application.

Recommended initialization parameters

Recommended init.ora settings for *Microsoft Windows* (assuming 24G RAM with 8 Core CPU Oracle server).

Name	Value	Description
`cursor_sharing`	`EXACT`	EXACT ensures that Oracle computes the most efficient execution plans. This causes a higher CPU consumption but a better performance on the execution. If the CPU consumption is to high, and the data size doesn't change significantly during the time, it may be a good idea to change it to FORCE. This ensures that the execution plans are reused and the CPU consumption remains low.
`db_block_checking`	`FALSE`	To avoid additional overhead.
`db_block_size`	`8192`	Default
`db_domain`		
`db_writer_processes`	`CPU cores / 8`	Oracle guideline.
`dynamic_sampling`	`2`	To enable dynamic sampling on tables without statistics (ReportStore/ReportStoreTemp).

Name	Value	Description
filesystemio_options	SETALL	
job_queue_processes	10	
nls_language	AMERICAN	
nls_territory	AMERICA	
open_cursors	3000	
optimizer_capture_sql_plan_baselines	FALSE	Setting this parameter to false will make SQL plan management to not recalculate the execution plan for each repeatable SQL statement.
optimizer_use_sql_plan_baselines	FALSE	Setting this parameter to false will make SQL plan management not to capture the history for the SQL statements being parsed or reparsed.
parallel_adaptive_multi_user	TRUE	
parallel_degree_limit	1	
processes	1000	Sufficient Oracle processes are allocated to support connection, parallel thread, internal process and other usage.
recyclebin	OFF	
remote_login_passwordfile	EXCLUSIVE	

Name	Value	Description
sessions	1000	
undo_management	AUTO	
tns_listener	TCP Protocol	
workarea_size_policy	AUTO	To be determined automatically by Oracle.

6.2.2.2 Database User Settings

During Product 360 schema installation you will need the **SYSTEM** user.

6.2.2.3 DBA Tasks

Your DBA must take care of the following topics:

- Always monitor I/O waits
- Redo Log Checkpoints/Switching
  - Frequent log switching decreases performance
  - Redo log size needs to be sized appropriately
- Archive Logs
  - When archive area is full, all processes in the DB stops until archive logs are backup and the archive backed up logs deleted to free up space
- Cache Hit Ratio
  - Should be at least a 95% cache hit

6.3 Server Database

The Server Database manual describes how to initially setup or update the Product 360 server database schemas for a new release.

- Custom Indexes (see page 36)
- Oracle RAC, Oracle ASM (Automated Storage Management) (see page 36)
- Minimum Oracle privileges (see page 40)
  - Normal installation (tablespaces and db users are not existing before install process) (see page 40)
  - Installation with restricted privileges (similar update) (see page 42)
- Binaries (see page 43)
  - Extract the database setup archive (see page 43)
  - Provide database connection settings (see page 43)
  - Creating/Updating schemas - Microsoft SQL Server (GUI) (see page 51)
  - Creating/Updating schemas - Oracle (GUI) (see page 53)

- Creating/Updating schemas (Headless) (see page 55)
- Troubleshooting (see page 55)

6.3.1 Custom Indexes

It is allowed for DBAs to create own, customer specific indexes in tables, as long as those are not unique and therefore only for performance reasons. Search scenarios of productive installations can not all be foreseen by the development team and therefore it might be necessary to create additional indexes. We strongly encourage you to create those using scripts, and to provide also a drop script for them.

> All custom indexes must be removed before you execute the database setup - or it might fail because table adjustments can't be done as long as indexes are there which the setup doesn't know.

You can customize the database setup by adding scripts to the corresponding extension point. This is a comfortable way to remove and recreate such customized indexes. See development guide on how to do this.

6.3.2 Oracle RAC, Oracle ASM (Automated Storage Management)

Please note that the standard database setup is not aware of complex tablespace setups which are typical for larger Oracle environments. Since the policies around those tablespaces are quite complex and differ from customer to customer, we recommend to create the tablespaces and users manually. The database setup will skip the user and tablespace creation part in case it recognizes that those elements are already there. For this, the users and tablespaces need to be named correctly otherwise the setup won't recognize them.

The following scripts use PIM_ as prefix and no suffix. You need to make sure that the server.properties file match. If you want to use a different pre/suffix, you need to adjust the scripts accordingly.

Username and Tablespace names need to be in capital letters and start with a latin character. Tablespace names must not be longer than 30 characters, that means **prefix + schema name + suffix must not be longer than 24 characters.**

Prefix `(db.default.schema.prefix)`	**Schema Name**	**Suffix** `(db.default.schema.suffix)`	**Username**	**Temp Tablespace**	**Data Tablespace**	**Index Tablespace**
PIM_	MAIN		PIM_MAIN	PIM_MAIN_TEMP	PIM_MAIN_DATA	PIM_MAIN_INDEX
PIM_	MASTER		PIM_MASTER	PIM_MASTER_TEMP	PIM_MASTER_DATA	PIM_MASTER_INDEX
PIM_	SUPPLIER		PIM_SUPPLIER	PIM_SUPPLIER_TEMP	PIM_SUPPLIER_DATA	PIM_SUPPLIER_INDEX

The following scripts are examples - they most likeley should be adapted to the needs of the customer. Especially in terms of initial and maximum size!

Example: MAIN Script

```
CREATE TEMPORARY TABLESPACE "PIM_MAIN_TEMP"
 TEMPFILE '+DATAGRP1/pimfhqa/tempfile/pim_main_temp.263.860573097'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1024K;

CREATE TABLESPACE "PIM_MAIN_DATA"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_main_data.264.860573159'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING
 EXTENT MANAGEMENT LOCAL
 SEGMENT SPACE MANAGEMENT AUTO;

CREATE TABLESPACE "PIM_MAIN_INDEX"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_main_index.265.860573217'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING
 EXTENT MANAGEMENT LOCAL
 SEGMENT SPACE MANAGEMENT AUTO;

CREATE USER "PIM_MAIN"
 PROFILE "DEFAULT"
 IDENTIFIED BY pimadmin
 DEFAULT TABLESPACE "PIM_MAIN_DATA"
 TEMPORARY TABLESPACE "PIM_MAIN_TEMP"
 ACCOUNT UNLOCK;
GRANT UNLIMITED TABLESPACE TO "PIM_MAIN";
GRANT "CONNECT" TO "PIM_MAIN";
GRANT "RESOURCE" TO "PIM_MAIN";
```

Example: MASTER Script

```
CREATE TEMPORARY TABLESPACE "PIM_MASTER_TEMP"
 TEMPFILE '+DATAGRP1/pimfhqa/tempfile/pim_master_temp.266.860574107'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1024K;

CREATE TABLESPACE "PIM_MASTER_DATA"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_master_data.267.860574173'
```

```
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING
 EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;

CREATE TABLESPACE "PIM_MASTER_INDEX"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_master_index.268.860574237'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;

CREATE USER "PIM_MASTER"
 PROFILE "DEFAULT"
 IDENTIFIED BY pimadmin
 DEFAULT TABLESPACE "PIM_MASTER_DATA"
 TEMPORARY TABLESPACE "PIM_MASTER_TEMP"
 ACCOUNT UNLOCK;
GRANT UNLIMITED TABLESPACE TO "PIM_MASTER";
GRANT "CONNECT" TO "PIM_MASTER";
GRANT "RESOURCE" TO "PIM_MASTER";
```

Example: SUPPLIER Script

```
CREATE TEMPORARY TABLESPACE "PIM_SUPPLIER_TEMP"
 TEMPFILE '+DATAGRP1/pimfhqa/tempfile/pim_supplier_temp.269.860574555'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1024K;

CREATE TABLESPACE "PIM_SUPPLIER_DATA"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_supplier_data.270.860574619'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING
 EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;

CREATE TABLESPACE "PIM_SUPPLIER_INDEX"
 DATAFILE '+DATAGRP1/pimfhqa/datafile/pim_supplier_index.271.860574685'
 SIZE 1024M REUSE
 AUTOEXTEND ON NEXT 1024M
 MAXSIZE 32767M
 LOGGING
 EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;

CREATE USER "PIM_SUPPLIER"
 PROFILE "DEFAULT"
```

```
  IDENTIFIED BY pimadmin
  DEFAULT TABLESPACE "PIM_SUPPLIER_DATA"
  TEMPORARY TABLESPACE "PIM_SUPPLIER_TEMP"
  ACCOUNT UNLOCK;
GRANT UNLIMITED TABLESPACE TO "PIM_SUPPLIER";
GRANT "CONNECT" TO "PIM_SUPPLIER";
GRANT "RESOURCE" TO "PIM_SUPPLIER";
```

6.3.3 Minimum Oracle privileges

6.3.3.1 Normal installation (tablespaces and db users are not existing before install process)

Normal installation means in this context that the tablespaces and also the needed database users for the server will be created while the installation process. The users and also the tablespace have to be defined in the configuration file server.properties.The database use which will run the installation procedures needs at minimum the following privileges.

Role	Granted	Admin
CONNECT	X	X
RESOURCE	X	X

System Privileges	Granted	Admin
CREATE USER	X	-
CREATE TRIGGER	X	-
CREATE TABLESPACE	X	-
CREATE SEQUENCE	X	-
CREATE TABLE	X	-
CREATE PROCEDURE	X	-

System Privileges	Granted	Admin
GRANT ANY PRIVILEGE	X	-
CREATE TYPE	X	-
ALTER USER	X	-
CREATE SESSION	X	-
UNLIMITED TABLESPACE	X	-
SELECT ANY DICTIONARY	X	-

Example: Database Install User Script

```
-- USER SQL
CREATE USER INFA_DB_INSTALLER IDENTIFIED BY "password" DEFAULT TABLESPACE "USERS"
TEMPORARY TABLESPACE "TEMP";
-- ROLES
GRANT "RESOURCE" TO INFA_DB_INSTALLER WITH ADMIN OPTION;
GRANT "CONNECT" TO INFA_DB_INSTALLER WITH ADMIN OPTION;
-- SYSTEM PRIVILEGES
GRANT CREATE USER TO INFA_DB_INSTALLER ;
GRANT CREATE TRIGGER TO INFA_DB_INSTALLER ;
GRANT CREATE TABLESPACE TO INFA_DB_INSTALLER ;
GRANT CREATE SEQUENCE TO INFA_DB_INSTALLER ;
GRANT CREATE TABLE TO INFA_DB_INSTALLER ;
GRANT CREATE PROCEDURE TO INFA_DB_INSTALLER ;
GRANT GRANT ANY PRIVILEGE TO INFA_DB_INSTALLER ;
GRANT CREATE TYPE TO INFA_DB_INSTALLER ;
GRANT ALTER USER TO INFA_DB_INSTALLER ;
GRANT CREATE SESSION TO INFA_DB_INSTALLER ;
GRANT UNLIMITED TABLESPACE TO INFA_DB_INSTALLER;
GRANT SELECT ANY DICTIONARY TO INFA_DB_INSTALLER ;
```

6.3.3.2 Installation with restricted privileges (similar update)

The installation can also be done with more restricted privileges but in this case the tablespaces and the database uesrs have to be created before the installation process by an Oracle DBA. See chapter "Oracle RAC, Oracle ASM (Automated Storage Management)" (see page 36).
The database use which will run the installation procedures needs at minimum the following privileges.

Role	Granted	Admin
CONNECT	X	-

System Privileges	Granted	Admin
CREATE TRIGGER	X	-
CREATE SEQUENCE	X	-
CREATE TABLE	X	-
CREATE PROCEDURE	X	-
GRANT ANY PRIVILEGE	X	-
CREATE TYPE	X	-
SELECT ANY DICTIONARY	X	-

Example: Database Install User Script

```
-- USER SQL
CREATE USER INFA_DB_INSTALL_USER IDENTIFIED BY "password" DEFAULT TABLESPACE
"PIM_MAIN_DATA" TEMPORARY TABLESPACE "PIM_MAIN_TEMP";

-- ROLES
```

```
GRANT "CONNECT" TO INFA_DB_INSTALL_USER;


-- SYSTEM PRIVILEGES
GRANT CREATE TRIGGER TO INFA_DB_INSTALL_USER ;
GRANT CREATE SEQUENCE TO INFA_DB_INSTALL_USER ;
GRANT CREATE TABLE TO INFA_DB_INSTALL_USER ;
GRANT CREATE PROCEDURE TO INFA_DB_INSTALL_USER ;
GRANT GRANT ANY PRIVILEGE TO INFA_DB_INSTALL_USER ;
GRANT CREATE TYPE TO INFA_DB_INSTALL_USER ;
GRANT SELECT ANY DICTIONARY TO INFA_DB_INSTALL_USER ;
```

6.3.4 Binaries

The database setup is distributed within the product core archive and has the following format `PIM_<Version>_<Revision>_dbSetupClient_win64.zip`

> The database setup currently cannot be executed from a Linux server. In order to install the database on a Linux server, the setup has to be executed remotely from a Windows computer. The settings have to be adjusted appropriately.

6.3.4.1 Extract the database setup archive

On the database server extract the `PIM_<Version>_<Revision>_dbSetupClient_win64.zip` to an installation root of your choice.
For this documentation we will choose `C:\INFORMATICA\PIM` (= `<PIM_DATABASE_INSTALLATION ROOT>`)

6.3.4.2 Provide database connection settings

Before running the database installation, some basic configuration needs to be done. The settings for the database connection are configured in the `server.properties` file. Templates for this file can be found in the configuration folder of the extracted archive.

> If you want to encrypt the database passwords in the configuration file please refer to chapter Encryption of secure information (see page 0) in the Server Database (see page 35) manual. The passwords marked as to encrypt will be encrypted during the database setup.
> Updating to newest Hotfix you should also replace the Java JCE policy files in `jre\lib\security` folder.

> If you want to connect the P360 Server to an Oracle Database via TCPS, please refer to chapter "How to configure a secure database connection for Product 360 Server" in the "Server Configuration" manual.

Perform the following steps to adjust the `server.properties` file:

1. Rename the appropriate template file **`<PIM_DATABASE_INSTALLATION ROOT>\<Version>_<Revision>_dbSetupClient_win64.zip\configuration\server.properties.template.[DBMS] to`** `server.properties`
2. Adjust the settings as described in the following table:

Property	Description
General Settings	
`repository.default.language`	The default language of the repository regarding all language specific aspects like e.g. default logical key language. Possible values: Key synonyms of the corresponding language entries defined in the repository enumeration " `Enum.Language` ", e.g. `"de"` or `"en_US"` - default is German, if property does not exist.
Database settings for Microsoft SQL Server (We only describe the default settings here. Most of those can be adjusted individually for each database schema as you will see in the server.properties template file. However, splitting the schemas on multiple database hosts/instances is not supported since there are cross schema sql statements which would not work!)	
`db.integrated.security`	If your security guidelines do not allow passwords in configuration files this preference allows you to use integrated authentication on Windows operating systems. "Integrated Security" is a security functionality of Microsoft SQL Server. If other password protection mechanism is used, then keep this setting in the configuration file and set to false.
`db.default.type`	`MSSQL` This property should never be changed!

Property	Description
`db.default.server`	The host name of the Microsoft SQL Server; Change this in case you have a separate database server
`db.default.port`	Port of the Microsoft SQL Server instance, usually this is 1433
`db.default.user`	User name of the database user (if integrated authentication is used this property can be empty)
`db.default.password`	Password of the database user (if integrated authentication is used this property can be empty)
`db.default.dir`	Base folder for the database schema and database transaction log files **Note: This folder needs not to be local to the application server but to the database server!**
`db.default.dir.data`	Folder for the database schema files (`*.mdf`)
`db.default.dir.log`	Folder for the transaction log files (`*.ldf`)
`db.default.data.size`	Default size in MB allocated for a database schema; adapt this setting to your needs

Property	Description
`db.default.data.size.growth`	Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs In a productive environment you should define the initial size of the database to the expected maximum. A data base growth action always "stops the world" of the database until the files are enlarged. In case the growth size is too small, this might occur very often which is a serious performance problem!
`db.main.pool.jdbcUrl`	**10.5.02.01 onwards** New connection property "encrypt=false" added in the url jdbc:sqlserver://${db.main.server}:${db.main.port};databaseName=${db.main.database};integratedSecurity=${db.integrated.security};sendStringParametersAsUnicode=true;selectMethod=direct;responseBuffering=adaptive**;encrypt=false**
`db.master.pool.jdbcUrl`	**10.5.02.01 onwards** New connection property "encrypt=false" added in the url jdbc:sqlserver://${db.master.server}:${db.master.port};databaseName=${db.master.database};integratedSecurity=${db.integrated.security};sendStringParametersAsUnicode=true;selectMethod=direct;responseBuffering=adaptive**;encrypt=false**
`db.supplier.pool.jdbcUrl`	**10.5.02.01 onwards** New connection property "encrypt=false" added in the url jdbc:sqlserver://${db.supplier.server}:${db.supplier.port};databaseName=${db.supplier.database};integratedSecurity=${db.integrated.security};sendStringParametersAsUnicode=true;selectMethod=direct;responseBuffering=adaptive**;encrypt=false**
`db.default.log.size`	Default size in MB allocated for a database transaction log file; adapt this setting to your needs

Property	Description
`db.default.log.size.growth`	Default increment value in MB allocated when space for a database transaction log file is insufficient; adapt this setting to your needs Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs In a productive environment you should define the initial size of the database log files to the expected maximum. A data base growth action always "stops the world" of the database until the files are enlarged. In case the growth size is too small, this might occur very often which is a serious performance problem!
`db.default.schema.prefix`	Usually, this property needs not to be changed. The common prefix for all server schemas; **it must be in capital, start with a latin character and must not contain any special characters except '_'!**
`db.default.schema.suffix`	Usually, this property needs not to be changed. The common suffix for all erver schemas; **it must be in capital, start with a latin character and must not contain any special characters except '_'!** This property is helpful to distinguish between productive and test schemas (e.g. `_PRO` and `_TEST`)
`db.default.debug.show_sql`	Usually, this property needs not to be changed. Generated SQL statements during runtime will be shown in the log file. This is a debugging feature which will slow down the application drastically if turned on.
`db.default.rowPrefetchSize`	Affects the default prefetch size which is especially important for mass data retrieval. In SQL Server there is usually no need to change that.
`db.default.pool.hibernate.dialect`	The corresponding dialect for your MSSQL version For MSSQL 2016: com.heiler.ppm.persistence.db.internal.dialect.SQLServer2016 For MSSQL 2014: com.heiler.ppm.persistence.db.internal.dialect.SQLServer2012

Property	Description
Database settings for Oracle (we only describe the default settings here. Most of those can be adjusted individually for each database schema as you will see in the server.properties template file. However, splitting the schemas on multiple database hosts/instances is not supported since there are cross schema sql statements which would not work!)	
`db.default.type`	`ORACLE` Never change this property!
`db.default.database`	Oracle Service Name(SID)
`db.default.server`	The host name of the Oracle server; change this in case you have a separate database server.
`db.default.port`	Port of the Oracle instance, usually this is 1521
`db.default.password`	Password for the created schema users
`db.default.dir`	Base folder for the database schema and database transaction log files **Note: This folder needs not to be local to the application server but to the database server!**
`db.default.dir.data`	Folder for the database schema files
`db.default.dir.temp`	Folder for the database transaction log files

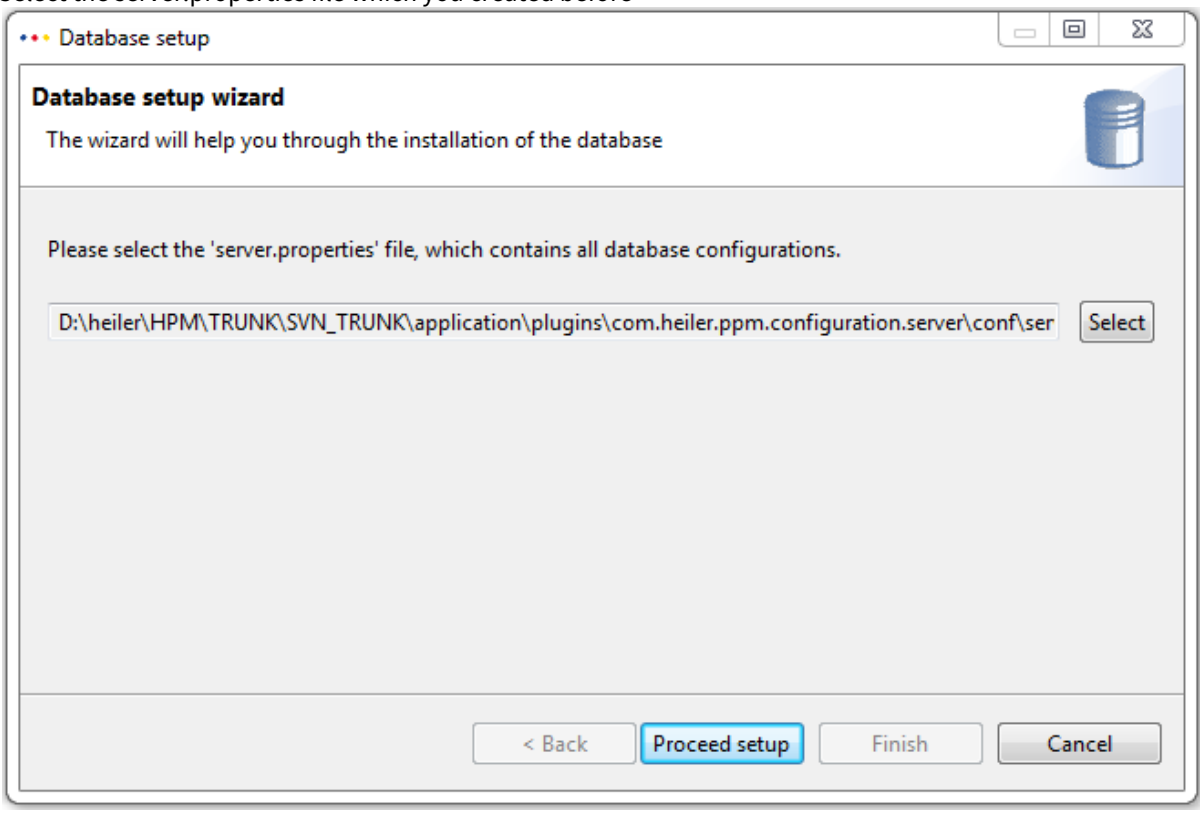
Property	Description
`db.default.dir.index`	Folder for the index tablespaces
`db.default.data.size`	Default size in MB allocated for a database schema; adapt this setting to your needs
`db.default.data.size.growth`	Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs In a productive environment you should define the initial size of the database log files to the expected maximum. A data base growth action always "stops the world" of the database until the files are enlarged. In case the growth size is too small, this might occur very often which is a serious performance problem!
`db.default.temp.size`	Default size in MB allocated for a database transaction log file; adapt this setting to your needs
`db.default.temp.size.growth`	Default increment value in MB allocated when space a transaction log file is insufficient; adapt this setting to your needs In a productive environment you should define the initial size of the database log files to the expected maximum. A data base growth action always "stops the world" of the database until the files are enlarged. In case the growth size is too small, this might occur very often which is a serious performance problem!
`db.default.index.size`	Default size in MB allocated for an index tablespace; adapt this setting to your needs

Property	Description
`db.default.index.size.growth`	Default increment value in MB allocated when space for an index tablespace is insufficient; adapt this setting to your needs In a productive environment you should define the initial size of the database log files to the expected maximum. A data base growth action always "stops the world" of the database until the files are enlarged. In case the growth size is too small, this might occur very often which is a serious performance problem!
`db.default.schema.prefix`	The common prefix for all server schemas; **it must be in capital, start with a latin character and must not contain any special characters except '_'! Note that the resulting tablespace name (prefix + <MAIN|MASTER|SUPPLIER> + suffix) must not be longer than 24 characters.**
`db.default.schema.suffix`	The common suffix for all server schemas; **it must be in capital, start with a latin character and must not contain any special characters except '_'! Note that the resulting tablespace name (prefix + <MAIN|MASTER|SUPPLIER> + suffix) must not be longer than 24 characters.** This property is helpful to distinguish between productive and test schemas (e.g. `_PRO` and `_TEST`).
`db.default.debug.show_sql`	Generated SQL statements during runtime will be shown in the log file. This is a debugging feature which will slow down the application drastically.
`db.default.rowPrefetchSize`	Affects the default prefetch size which is especially important for mass data retrieval. This value might be modified in case you have a lot of memory. The oracle driver is allocating the complete, theoretically needed memory for a single round trip. In case you run into memory problems because of the Oracle database access, you might want to decrease this property. See also the How to enable Java Management Extensions (JMX).

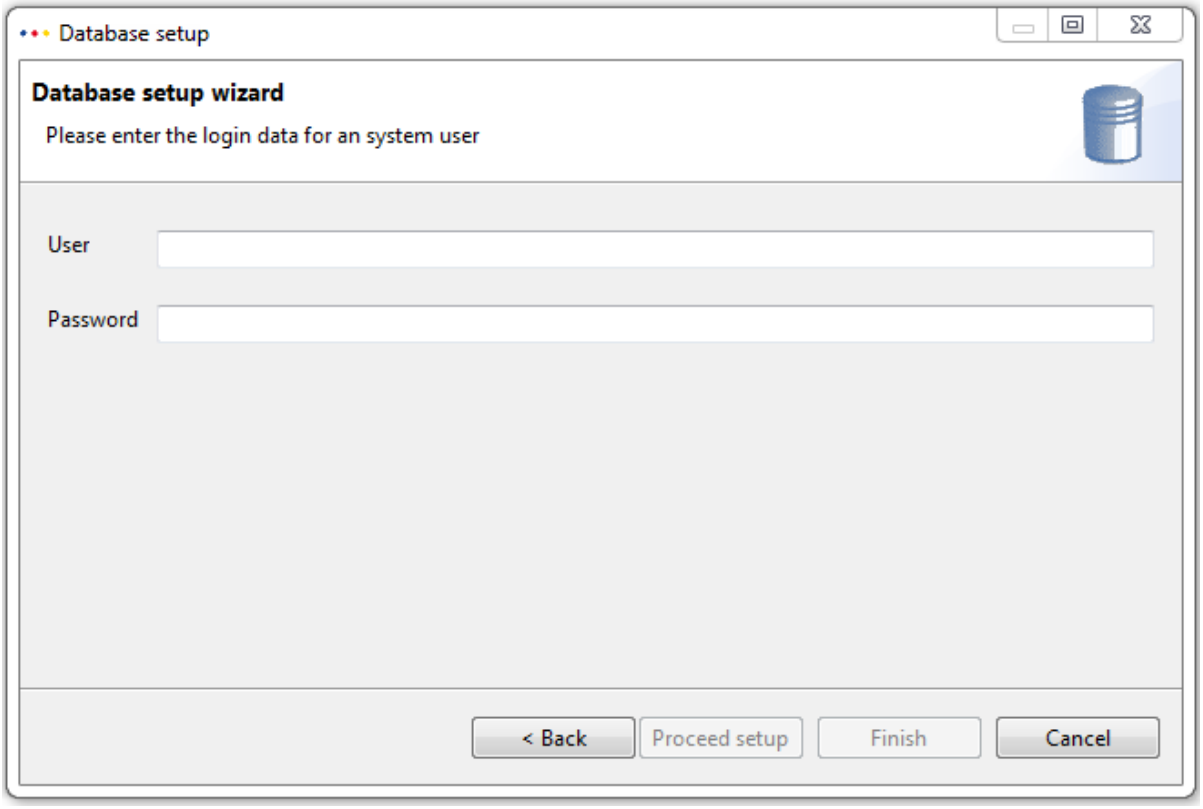
Property	Description
`db.default.pool.hibernate.dialect`	The corresponding dialect for your Oracle version. Currently only one value, no need to change. com.heiler.ppm.persistence.db.internal.dialect.Oracle12c

6.3.4.3 Creating/Updating schemas - Microsoft SQL Server (GUI)

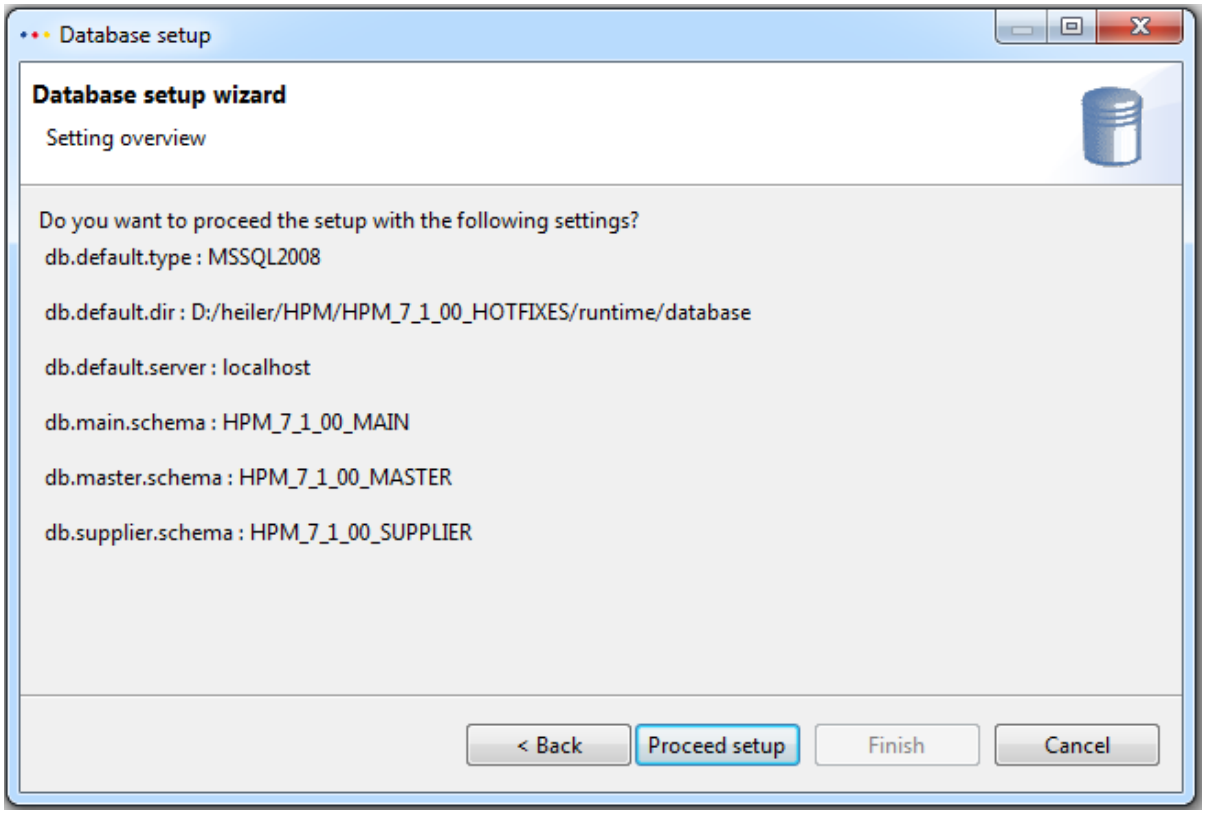
1. Start the database setup with a double click on **`Database.exe`** file. The wizard will open
2. Select the server.properties file which you created before



3. In case you want to create/update an Oracle database, you will have to provide the credentials of a user which has DB Admin rights. For example, the SYSTEM user.



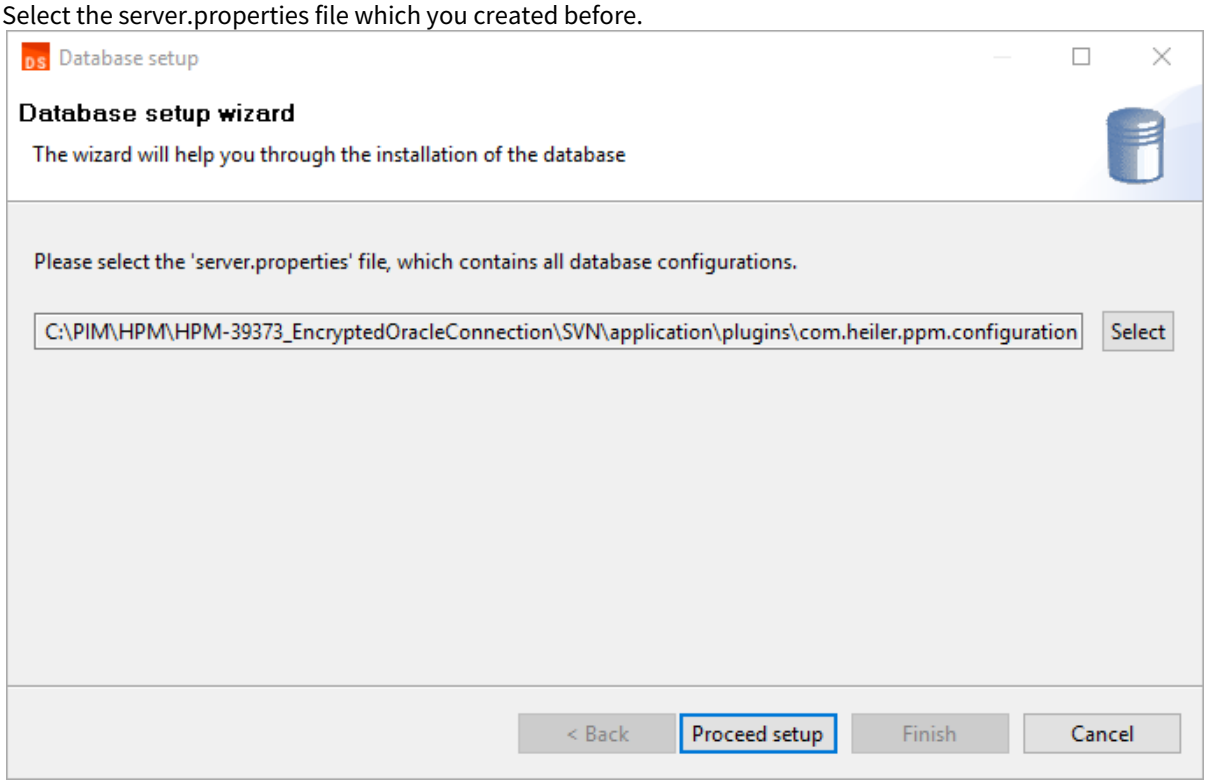
4. After clicking Proceed setup you will get an overview of some settings of the server.properties file you selected.



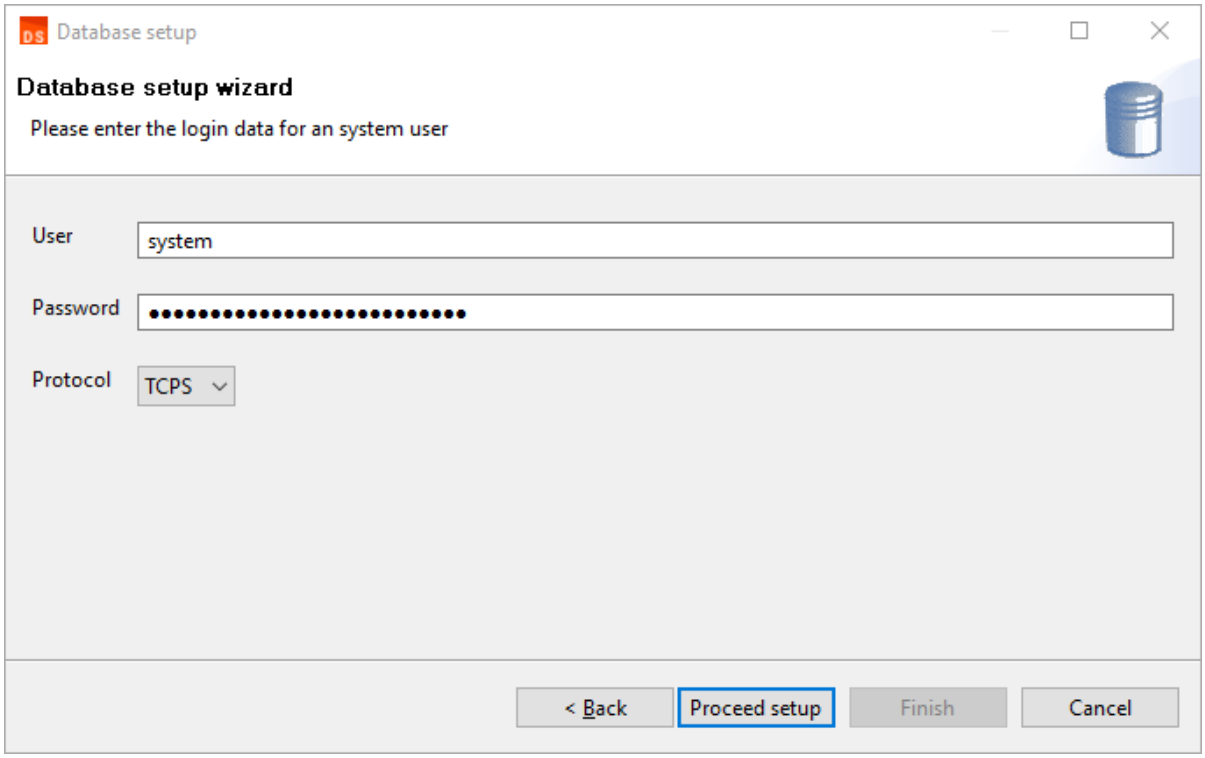
5. By clicking `Proceed setup` the database will be created/updated with the settings defined by the server.properties file
6. In case of an exception, the setup will be aborted and the cause will be shown. After resolving the problem, the setup can be executed again. It will continue at the point where it was aborted. This is achieved by some checkings against the database.
7. The log files contain all steps which where executed and in case of an exception the stack trace can be found here. If the exception is caused by a sql query, the exact query which was sent to the database will be logged too.

6.3.4.4 Creating/Updating schemas - Oracle (GUI)

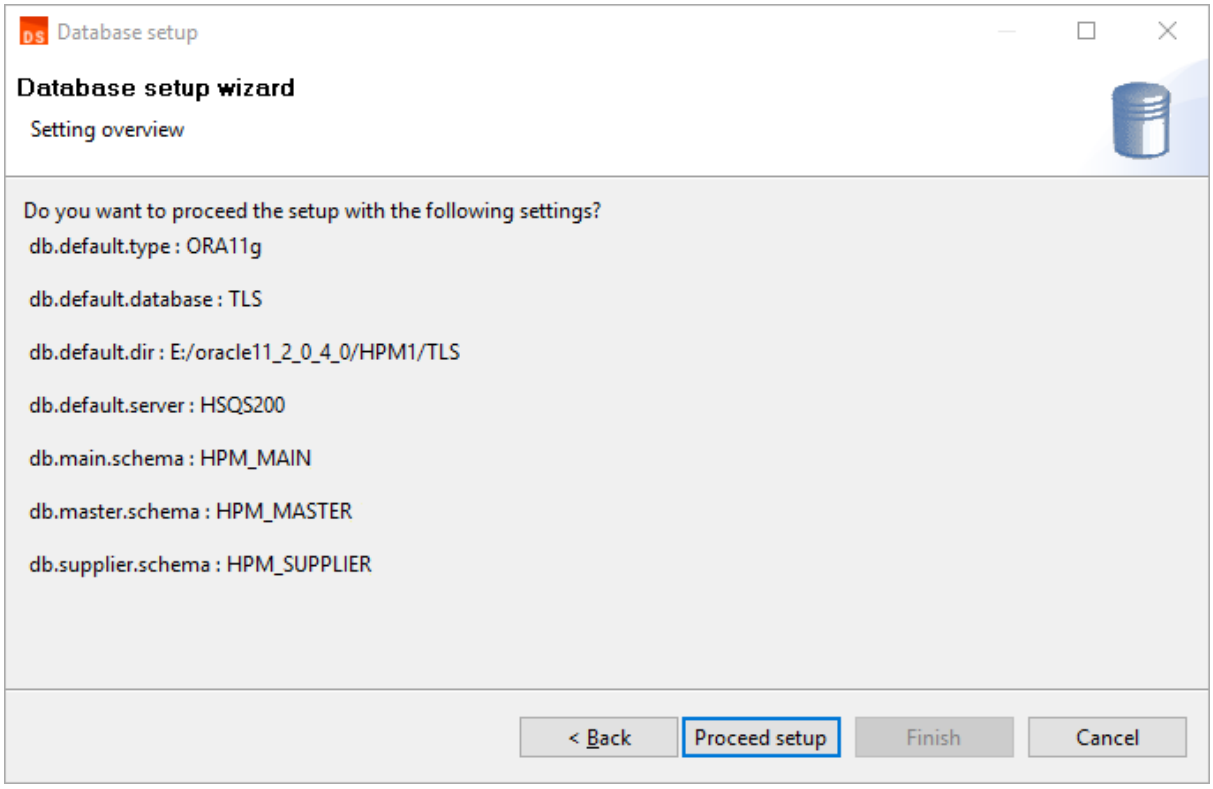
1. Start the database setup with a double click on **`Database.exe`** file. The wizard will open.
2. Select the server.properties file which you created before.



3. In case you want to create/update an Oracle database, you will have to provide the credentials of a user which has DB Admin rights. For example, the SYSTEM user. You will also have to choose wether you want to use a `TCP` or a `TCPS` connection.



4. After clicking Proceed setup you will get an overview of some settings of the server.properties file you selected.



5. By clicking `Proceed setup` the database will be created/updated with the settings defined by the server.properties file

6. In case of an exception, the setup will be aborted and the cause will be shown. After resolving the problem, the setup can be executed again. It will continue at the point where it was aborted. This is achieved by some checkings against the database.
7. The log files contain all steps which where executed and in case of an exception the stack trace can be found here. If the exception is caused by a sql query, the exact query which was sent to the database will be logged too.

6.3.4.5 Creating/Updating schemas (Headless)

1. Open a console and navigate to the extracted package where the database.exe file is located
2. Execute the setup by entering '`database -application com.heiler.ppm.dbsetup.core.app -consoleLog -noExit <full path to server.properties>`'
3. If you like to create/update an Oracle db, you have to specify also a user and password right after the server.properties file path perameter.
4. For a detailed information on the params simply enter '`database -application com.heiler.ppm.dbsetup.core.app -noExit help`'

> In case local policies do not allow the automatic creation of database schemas, or on case of a more complex setup of tablespaces, DBAs can create the empty schemas manually. They need to make sure that the configured users exist and have privileges on the schemas. The setup will recognize that the tablespaces / schemas already exist and will use them.

6.3.5 Troubleshooting

We can't guarantee that the schema setup will run without any issues in case of a migration of old schemas.

This has several reasons:

- Existence of customer specific indexes -> These will break automatic extension / change of table structure if not removed prior to the database setup
- Missing user rights of db user -> This will lead to a stopped execution of db setup
- Some technical limitation which appears especially in cross schema modifications -> Can happen especially during migrations of schemas which are older than version 7

In case of an exception the setup will be stopped and the error shown. Try to solve the issue and restore your backup and execute the setup fresh. **Please do not just restart the setup since depending on the error which occured we can not guarantee a consistent state of the database.**

6.4 Media Manager Database

- Installing the Media Manager database (see page 56)
- Oracle specific information (see page 58)
  - Create tablespaces manually for Oracle RAC, Oracle ASM (Automated Storage Management) (see page 58)

    - Minimum Oracle privileges (see page 59)
- Microsoft SQL Server specific information (see page 61)
    - Operating the application without db_owner role (see page 62)
    - Operating the application without database user "OPASPUBLIC" (see page 63)
    - Installing full-text search for Microsoft SQL Server (see page 64)
    - Activating further iFilters on Microsoft SQL Server 2008 (see page 65)
- Post-flight steps (see page 66)

6.4.1 Installing the Media Manager database

> **Important**
>
> Please ensure that the "Microsoft Visual C++ 2010 Redistributable" package is installed! If it's not installed you can download it from the Microsoft download page or you run the client installation program (see: Installing the client modules (see page 120)) which automatically installs this package.

> **Oracle initializing parameter for the database configuration**
>
> Database character set: AL32UTF8
> Country specific character set: UTF8 – Unicode 3.0
> Standard language: American
> Standard date format: USA

To install the Product 360 - Media Manager database, you require the file **PIM_<Version>_MediaManager.zip** from your Product 360 distribution.
The procedure for installing your Product 360 - Media Manager database is as follows:

1. Uncompress the file **PIM_<Version>_MediaManager.zip** on your Windows computer.
2. Navigate to the folder **\MAIN_DVD\Setup\win\install database** of the uncompressed archive.
3. Remove the write protection of the copied folder and its subfolders.
4. Run the program **IMM__ins.exe**.
5. Select a folder in which you want to save the log file.
6. Select the type of the destination database (MSSQL or Oracle).
7. Enter the password assigned to the user sys during Oracle installation or the password assigned to the user sa during the MSSQL installation.

   > **MSSQL connection with Domain Account**
   >
   > You can use also a Windows Domain account to install the database. This account must be configured in the ODBC connection. In this case leave username and password empty. (Available with 8.0.6 Hotfix 4)

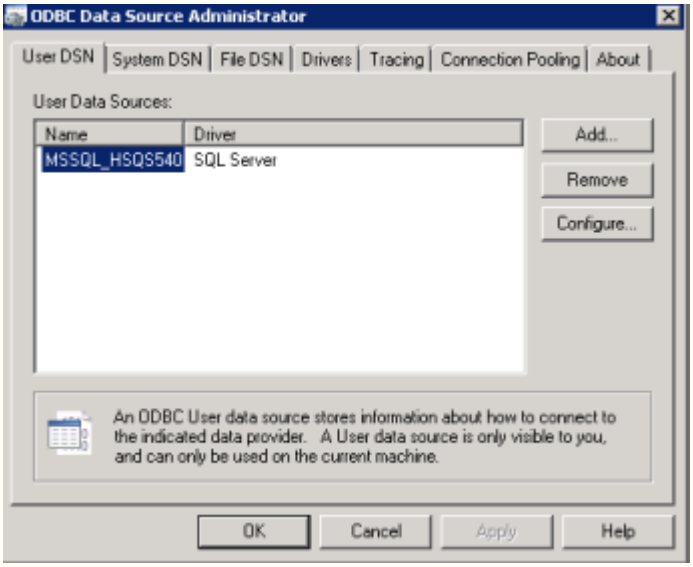
8. Enter host string for your database.

   > **Important for Oracle**

Please make sure that you installed the Oracle instant client software to connect to an existing oracle database. The easiest way to install this software is to install the Product 360 - Media Manager modules (see: Installing the client modules (see page 120)).
An example for the host string is: //HSQS540:1521/IMM

Important for Microsoft SQL Server

The host string has to start with MSSQL and it has to be defined as an ODBC connection in the register User DSN.



Go through the configurations wizard and set database host, credentials and default database.

If you want to create the tablespaces manually for Oracle RAC/ASM support then see next chapter Create tablespaces manually for Oracle. (see page 58) This will skip the table space creation process in installation programm and start the content installation directly.

9. You may now change the password for Product 360 - Media Manager database user OPASUSER.
10. Oracle ony: Enter the size and absolute path for the OPASALL table space.

    The recommended file name is opasall1.dbf. The recommended size is 750 MB.

11. Oracle only: Click on **Create** to create the table space.
12. Oracle only: Repeat this procedure for the table spaces OPASPRD and OPASIMG.

    The recommended file names are opasprd1.dbf and opasimg1.dbf. The recommended size is 1 GB each.

13. Oracle only: You will see a message confirming that the table spaces have been created and the database content has been transferred.
14. Oracle only: Acknowledge this message by clicking on **OK**.
15. Now view the Database installation log and acknowledge it by clicking on **OK**.

> You can view all the relevant entries again later in the log file, which is located in the installation directory.

6.4.2 Oracle specific information

6.4.2.1 Create tablespaces manually for Oracle RAC, Oracle ASM (Automated Storage Management)

To support Oracle RAC / ASM it is possible to create the Media Manager tablespaces manually. The database setup will skip the user and tablespace creation part in case it recognizes that those elements are already there. For this, the users and tablespaces need to be named correctly otherwise the setup won't recognize them. The following script shows an example how these tablespaces (OPASALL, OPASIMG and OPASPRD) can be created.

Example Script

```
CREATE TABLESPACE "OPASALL"
 LOGGING
 DATAFILE '+DATAGRP1/pimfhqa/datafile/opasall.297.860648937'
 SIZE 1024M
 AUTOEXTEND ON NEXT 250M
 MAXSIZE UNLIMITED
 EXTENT MANAGEMENT LOCAL SEGMENT
 SPACE MANAGEMENT AUTO;

CREATE TABLESPACE "OPASIMG"
 LOGGING
 DATAFILE '+DATAGRP1/pimfhqa/datafile/opasimg.298.860648958'
 SIZE 512M
 AUTOEXTEND ON NEXT 250M
 MAXSIZE UNLIMITED
 EXTENT MANAGEMENT LOCAL SEGMENT
 SPACE MANAGEMENT AUTO;

CREATE TABLESPACE "OPASPRD"
 LOGGING
 DATAFILE '+DATAGRP1/pimfhqa/datafile/opasprd.299.860648972'
 SIZE 512M
 AUTOEXTEND ON NEXT 250M
 MAXSIZE UNLIMITED
 EXTENT MANAGEMENT LOCAL SEGMENT
 SPACE MANAGEMENT AUTO;
```

6.4.2.2 Minimum Oracle privileges

Role	Granted	Admin	Default	Mandatory
CONNECT	X	X	X	X
RESOURCE	X	X	X	X
CTXAPP	X	X	-	-

System Privileges	Granted	Admin
CREATE USER	X	-
CREATE TRIGGER	X	X
CREATE TABLESPACE	X	X
CREATE TABLE	X	X
CREATE ANY INDEX	X	-
GRANT ANY OBJECT	X	-
CREATE VIEW	X	X
CRETE ROLE	X	-
ALTER USER	X	X

System Privileges	Granted	Admin
CREATE ANY TABLE	X	-
UNLIMITED TABLESPACE	X	X
SELECT ANY DICTIONARY	X	-
CREATE PROFILE	X	-
ALTER SESSION	X	X

Object Privileges	Grant option
SELECT ON SYS.V_$SESSION	X
SELECT ON SYS.ALL_INDEXES	X
SELECT ON SYS.V_$DATABASE	X
SELECT ON SYS.DBA_TABLESPACES	X

Example User Create

```
-- USER SQL

CREATE USER INFA_IMM_DBINSTALL IDENTIFIED BY "password" DEFAULT TABLESPACE "USERS"
TEMPORARY TABLESPACE "TEMP";


-- ROLES
```

```
GRANT "RESOURCE" TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT "CTXAPP" TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT "CONNECT" TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
ALTER USER INFA_IMM_DBINSTALL DEFAULT ROLE "RESOURCE","CONNECT";

-- SYSTEM PRIVILEGES
GRANT CREATE USER TO INFA_IMM_DBINSTALL ;
GRANT CREATE TRIGGER TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT CREATE TABLESPACE TO INFA_IMM_DBINSTALL ;
GRANT CREATE TABLE TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT CREATE ANY INDEX TO INFA_IMM_DBINSTALL ;
GRANT GRANT ANY OBJECT PRIVILEGE TO INFA_IMM_DBINSTALL ;
GRANT CREATE VIEW TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT CREATE ROLE TO INFA_IMM_DBINSTALL ;
GRANT ALTER USER TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT CREATE ANY TABLE TO INFA_IMM_DBINSTALL ;
GRANT UNLIMITED TABLESPACE TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;
GRANT SELECT ANY DICTIONARY TO INFA_IMM_DBINSTALL ;
GRANT CREATE PROFILE TO INFA_IMM_DBINSTALL ;
GRANT ALTER SESSION TO INFA_IMM_DBINSTALL WITH ADMIN OPTION;

-- OBJECT PRIVILEGES
GRANT SELECT ON SYS.V_$SESSION TO INFA_IMM_DBINSTALL with grant option;
GRANT SELECT ON SYS.ALL_INDEXES TO INFA_IMM_DBINSTALL with grant option;
GRANT SELECT ON SYS.V_$DATABASE TO INFA_IMM_DBINSTALL with grant option;
GRANT SELECT ON SYS.DBA_TABLESPACES TO INFA_IMM_DBINSTALL with grant option;
```

Secure connection to Oracle

Using a secure connection to Oracle is supported. Please note that it is necessary to distribute the server's certificate on the client machines where you wish to establish a secure connection to Oracle. For details on secure connection configuration please refer to the corresponding manuals provided by Oracle.

6.4.3 Microsoft SQL Server specific information

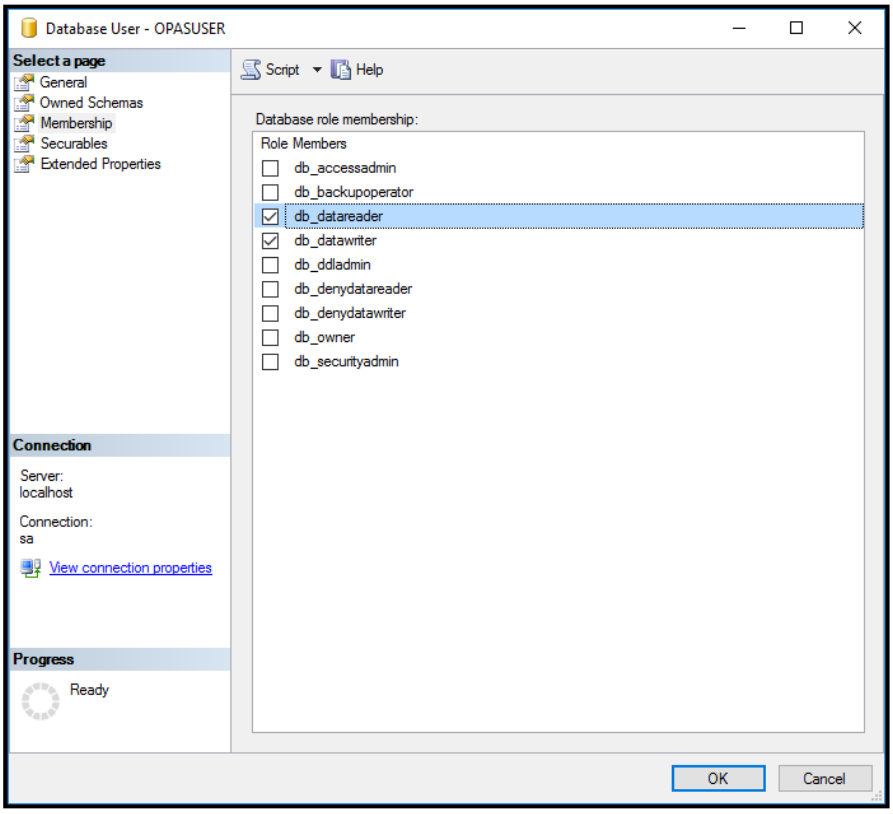
The mimimum privileges for the user wich installs the database are:

Permission	With grant
ALTER ANY LOGIN	-
CONNECT SQL	-
CREATE ANY DATABASE	-

Permission	With grant
VIEW ANY DATABASE	-
VIEW SERVER STATE	X

6.4.3.1 Operating the application without db_owner role

If your company policy prescribe a limited database access for application users it is possible to restrict the access of the database user "**OPASUSER**" to the roles: db_datareader and db_datawriter.



Update or Hotfix

While the update or hotfix process you have to grant the db_owner role temporary again to the user "OPASUSER" till this process is finished. Plese do not remove this role until at leaset one IMM module was started (e.g. Administration).

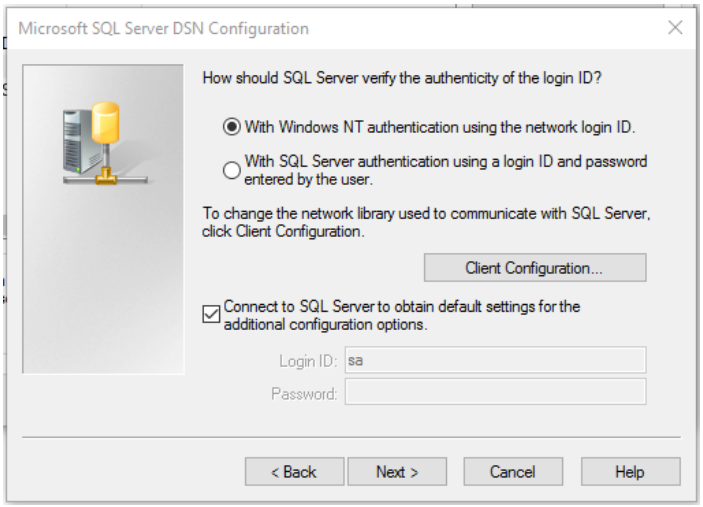
6.4.3.2 Operating the application without database user "OPASPUBLIC"

The Media Manager application works with a predefined database user "OPASPUBLIC". It is not possible to modify the hardcoded password of this user. If this violates aiaginst you company policy you have the possibilty to work with domain accounts. How to confiugre this will be described below.

Required access for the domain users in the Media Manager database:

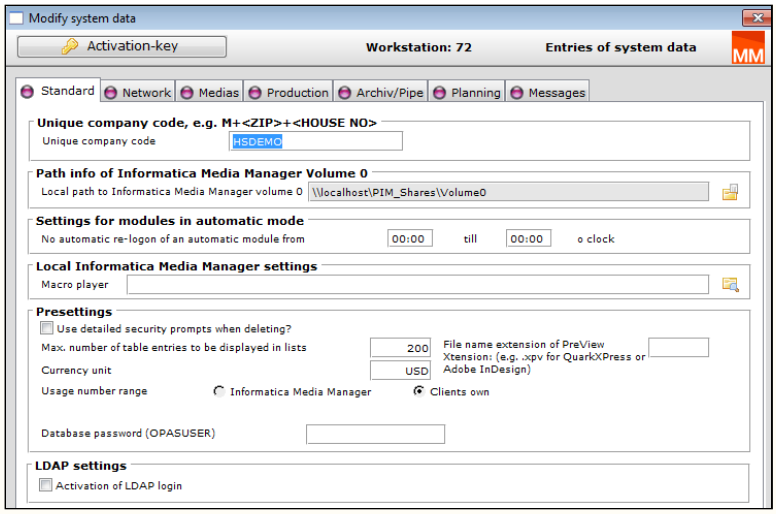
Table	Permission
dbo.O_DEFAULTS	Select
dbo.O_DEFAULTS	Update
dbo.O_DEFAULTS	Insert

Define the domain user for the ODBC connection.



Now it is safe to lock the user "OPASPUBLIC", but keep in my mind that you have to work with domain users in your ODBC connections on all workstations which uses the Media Manager applications.

> **OPASUSER Password**
>
> The password of the database user OPASUSER can only be changed within the MediaManager.Adminstion module. If you change it mnual for eaxample in the SQL server management studio the application will not work.



6.4.3.3 Installing full-text search for Microsoft SQL Server

> Microsoft SQL Server can create a full-text index only on data that exist in the database; i.e. the data that is to be indexed must be copied completely in the database. This means that with large files the database files grow accordingly.
> Microsoft SQL server can indicate all data types, for which the operating system can execute a full-text search in the Windows Explorer. The engines used for this purpose are called "iFilter". If the full-text search is to be extended for further data types, the appropriate iFilter has to be installed, e.g. for PDF the iFilter by Adobe.

To install the full-text search under Microsoft SQL Server, carry out the steps described below:

1. Open Microsoft SQL Server Management Studio.
2. Log on as administrator (user sa).
3. Navigate to **[database server name]/Databases/opasdsb/Tables**.
4. Choose **New Table...** at the context menu of the table list.
5. Define following columns for the table:

Column Name	Data Type	Allow Nulls
PKONT_PNR	nvarchar(20)	NO
DATEINAME	nvarchar(2000)	NO
PKONT_EXT	nvarchar(50)	NO

Column Name	Data Type	Allow Nulls
PKONT_CONTENT	varbinary(MAX)	YES

6. Define PKONT_PNR as Primary Key by clicking on the **Set Primary Key** Button at the menu bar.
7. Click on the **Save** Button at the menu bar.
8. Enter **F_IMGKONT** as table name.
9. Click on **OK**.

> Instead of performing the steps 4-9 you can run the create table F_IMGKONT.sql SQL script. You find the script in the **PIM_<Version>_MediaManager.zip** archive in the **manual/MSSQL directory**.

10. Mark **Tables** at the Object Explorer and click on the **Refresh** button.
11. Mark the F_IMGKONT table at the Object Explorer and choose **Full-Text index > Define Full-Text Index** at the context menu.
12. The wizard for installing the full-text search opens.
13. Click on **Next**.
14. At the first step the PK_F_IMGKONT index is already chosen; click on **Next**.
15. At the second step mark the PKONT_CONTENT column by clicking at the check box on the left.
16. Choose PKONT_EXT under the **Type** Column.
17. Click on **Next**.
18. At the third step leave the setting on **Automatically** and click on **Next**.
19. At the fourth step enter the name and location of the full-text catalog.
    - Name: F_IMGKONT
    - Location: If possible the full-text catalog should be for performance reasons on another hard disk. (This option is not available on MS SQL Server 2008 R2.)
20. Click on **Next**.
21. At the fifth step, click on **Next** without any changes.
22. At the last step you see a summary; click on **Finish.**
23. Execute the F_IMGKONT_UPLOADER.sql script to install the trigger. You find the script on your Product 360 - Media Manager DVD at the manual\MSSQL scripts folder.
24. Add the bulkadmin role to the user OPASUSER by executing the following SQL script: EXEC master..sp_addsrvrolemember @loginame = N'OPASUSER', @rolename = N'bulkadmin'GO Alternatively you can run the OPASUSER bulkadmin role.sql SQL script. You find the script on your Product 360 - Media Manager DVD at the manual/MSSQL scripts directory.

> The full-text search is activated at the customer in the Administration. This is only possible if you have a corresponding license and an existing F_IMGKONT table.

6.4.3.4 Activating further iFilters on Microsoft SQL Server 2008

If you have installed a further iFilter (e.g. Adobe PDF iFilter) you have to enable your Microsoft SQL Server for calling that iFilter.

1. Open the Microsoft SQL Server Management Studio.
2. Log on as administrator (user sa).
3. Open a new query.
4. Execute the following commands:

- Update the OS resources: **EXEC sp_fulltext_service @action='load_os_resources', @value=1**
- Disable signature verification: **EXEC sp_fulltext_service 'verify_signature', 0**
- Update the language list: **EXEC sp_fulltext_service 'update_languages'**
- Restart the daemon: **EXEC sp_fulltext_service 'restart_all_fdhosts'**
- If you want to check what iFilters are active execute this command: **EXEC sp_help_fulltext_system_components 'filter'**

6.4.4 Post-flight steps

After you've performed the database setup you also have to run the database update. This is done by the first startup of P360 Server, Media Manager web application or the Process Engine automatically by default.

If you've turned off the automatic update in Product 360 Server, the Media Manager web application or the Process Engine, or if you're not using one of those please refer to this chapter for database update instructions: Media Manager Migration

6.5 Supplier Portal Database

- Download the Product 360 Supplier Portal install file (see page 66)
- Create your Database Installation Root (see page 67)
- Setup initial database by install script (see page 67)
- Alternatively: Setup custom database manually (see page 73)

The Product 360 Supplier Portal needs its own data storage. It is recommended to use the same database server as for Product 360 Server, however, this is not mandatory.

Supplier Portal supports the standard DBMS Oracle and MS SQL Server. For non-productive environments (e.g. local development or demo purposes), a H2 database (http://www.h2database.com/) can also be used. Please note that H2 is not meant to be used in productive environments by design.

There are two ways to install the Supplier Portal database:

- An automatic installation script which installs a database with default settings. This is recommended for most scenarios.
- Alternatively, the manual installation guide for custom database setup. This can be used if specific requirements exists, e.g. the installation in an Oracle RAC infrastructure.

> All necessary database tables and indices are created during the first application bootstrap. No additional scripts need to be executed. Internally, the framework flyway is used for database setup and migrations.
>
> Supplier Portal uses the workflow engine Activiti that uses its own persistence. The Activiti tables are created (and updated) during the application bootstrap as well. No additional scripts are needed.

6.5.1 Download the Product 360 Supplier Portal install file

The package is part of the Product 360 installation package and named PIM_8.0.xx_SupplierPortal.zip.

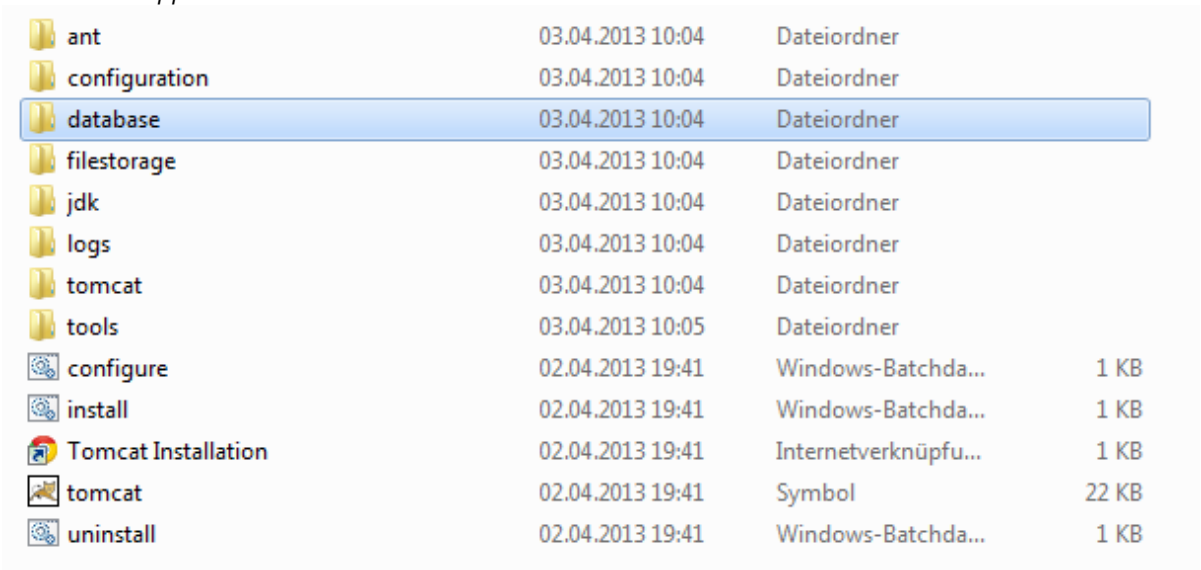
6.5.2 Create your Database Installation Root

Perform the following instructions to extract the database setup archive.

1. Unzip the **PIM_<*Version*>_SupplierPortal.zip** to an installation root of your choice.
   (in our example: **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT> =** *C:\INFORMATICA\PIM\SupplierPortal*)

   Check if the following folder structure under the installation root exists afterwards

   Screenshot: Supplier Portal Folder Structure



ant	03.04.2013 10:04	Dateiordner	
configuration	03.04.2013 10:04	Dateiordner	
database	03.04.2013 10:04	Dateiordner	
filestorage	03.04.2013 10:04	Dateiordner	
jdk	03.04.2013 10:04	Dateiordner	
logs	03.04.2013 10:04	Dateiordner	
tomcat	03.04.2013 10:04	Dateiordner	
tools	03.04.2013 10:05	Dateiordner	
configure	02.04.2013 19:41	Windows-Batchda...	1 KB
install	02.04.2013 19:41	Windows-Batchda...	1 KB
Tomcat Installation	02.04.2013 19:41	Internetverknüpfu...	1 KB
tomcat	02.04.2013 19:41	Symbol	22 KB
uninstall	02.04.2013 19:41	Windows-Batchda...	1 KB

6.5.3 Setup initial database by install script

The setup script requires a database command-line tool in the windows PATH environment variable:

- in case of Oracle this is *sqlplus*
- while MS SQL Server uses *sqlcmd*

Because of this, it's recommended to execute the setup script on the database server. Another pre-requisite is a JRE and a ANT distribution which both comes within the **PIM_<*Version*>_SupplierPortal.zip**.

6.5.3.1 Configure the database properties in the configuration.properties file

Before running the database installation, some basic configuration needs to be done. All database configuration properties can be found under the location

<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/configuration/configuration.properties.

For the database installation the following aspects need special attention:

MSSQL Installation:

Just uncomment and change the appropriate template settings in the configuration.properties.

Database settings	
`database.type`	Type of DBMS `mssql`
`database.name`	Name of the database, which will be created by the script `e.g. database.name=hsx_1.4`
`database.server`	Hostname of the database server `e.g. database.server=localhost`
`database.port`	Port number of the database server `default is database.port=1433`
`database.username`	Database user which needs dbcreator and public permissions `e.g. database.username=hsx`
`database.password`	password for the above specified database user
`database.data.dir`	Specifies the operating-system path to the database data file.
`database.data.size`	Is the initial size of the database data file. The kilobyte (KB), megabyte (MB), gigabyte (GB), or terabyte (TB) suffixes can be used. The default is MB. Specify a whole number; do not include a decimal. The minimum value for *size* is 512 KB.

`database.data.size.growth`	Specifies the growth increment of the databases data file. It is the amount of space added to the database data file each time new space is needed. Specify a whole number; do not include a decimal. A value of 0 indicates no growth. The value can be specified in MB, KB, GB, TB, or percent (%). If a number is specified without an MB, KB, or % suffix, the default is MB. When % is specified, the growth increment size is the specified percentage of the size of the database data file at the time the increment occurs.
`database.log.dir`	Specifies the operating-system path to the database log file.
`database.log.size`	Is the initial size of the database log file. The kilobyte (KB), megabyte (MB), gigabyte (GB), or terabyte (TB) suffixes can be used. The default is MB. Specify a whole number; do not include a decimal. The minimum value for *size* is 512 KB.
`database.log.size.growth`	Specifies the growth increment of the databases log file. It is the amount of space added to the database log file each time new space is needed. Specify a whole number; do not include a decimal. A value of 0 indicates no growth. The value can be specified in MB, KB, GB, TB, or percent (%). If a number is specified without an MB, KB, or % suffix, the default is MB. When % is specified, the growth increment size is the specified percentage of the size of the database log file at the time the increment occurs.

Oracle Installation:

Just uncomment and change the appropriate template settings in the configuration.properties.

Database settings	
`database.type`	Type of DBMS `oracle`
`database.name`	In case of oracle the database.name property is the SID or Service Name of the oracle database `e.g. database.name=XE`

`database.server`	Hostname of the database server `e.g. database.server=localhost`
`database.port`	Port number of the database server `default is database.port=1521` If you want to connect P360 Supplier Portal to an Oracle Database via TCPS, please refer to chapter "How to configure a secure database connection for Product 360 Supplier Portal" in the "Supplier Portal Configuration" manual.
`database.username`	Database user which needs dbcreator and public permissions `e.g. database.username=hsx`
`database.password`	password for the above specified database user
`database.systemUser`	**DON'T FORGET** User which has the permission to create other users/ tablespaces, is needed only to run the database creation script, feel free to remove this property after successfull script execution. `e.g. database.systemUser=SYSTEM`
`database.systemUser.password`	password for the above specified database system user
`database.data.dir`	Specifies the operating-system path to the database data file.
`database.data.size`	Specify the size of the database data tablespace file in bytes. Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes. Specify a whole number; do not include a decimal.

`database.data.size.growth`	specify the size in bytes of the next increment of disk space to be allocated automatically when more extents are required.Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes.Specify a whole number; do not include a decimal.
`database.temp.dir`	Specifies the operating-system path to the database temporary tablespace file.
`database.temp.size`	Specify the size of the database temporary tablespace file in bytes. Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes. Specify a whole number; do not include a decimal.
`database.temp.size.growth`	specify the size in bytes of the next increment of disk space to be allocated automatically when more extents are required. Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes.Specify a whole number; do not include a decimal.
`database.index.dir`	Specifies the operating-system path to the database index tablespace data file.
`database.index.size`	Specify the size of the database index tablespace data file in bytes. Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes. Specify a whole number; do not include a decimal.
`database.index.size.growth`	specify the size in bytes of the next increment of disk space to be allocated automatically when more extents are required. Use `K`, `M`, `G`, or `T` to specify the size in kilobytes, megabytes, gigabytes, or terabytes.Specify a whole number; do not include a decimal.

6.5.3.2 Execute Setup.cmd script

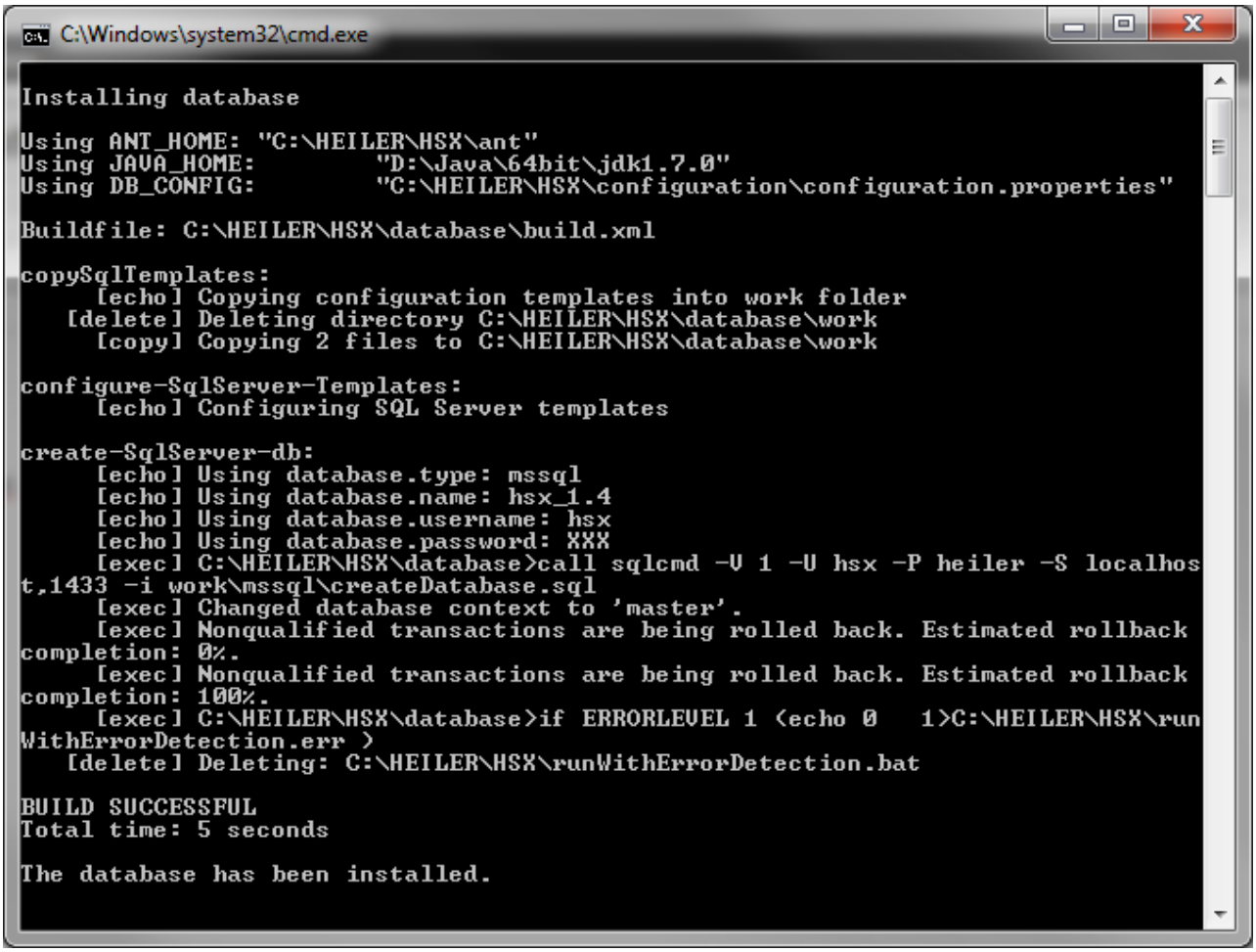
The database scripts are executed using ANT. The SQL template files can be found in /database/templates/mssql/createDatabase.sql and /database/templates/oracle/createDatabase.sql.

In most cases, the default settings should fit your needs. However, the scripts can be changed to adopt to the specific system environment. Please consult the Product 360 Server Database guide (see page 35) for an example how to configure Oracle ASM/RAC compatible tablespaces.

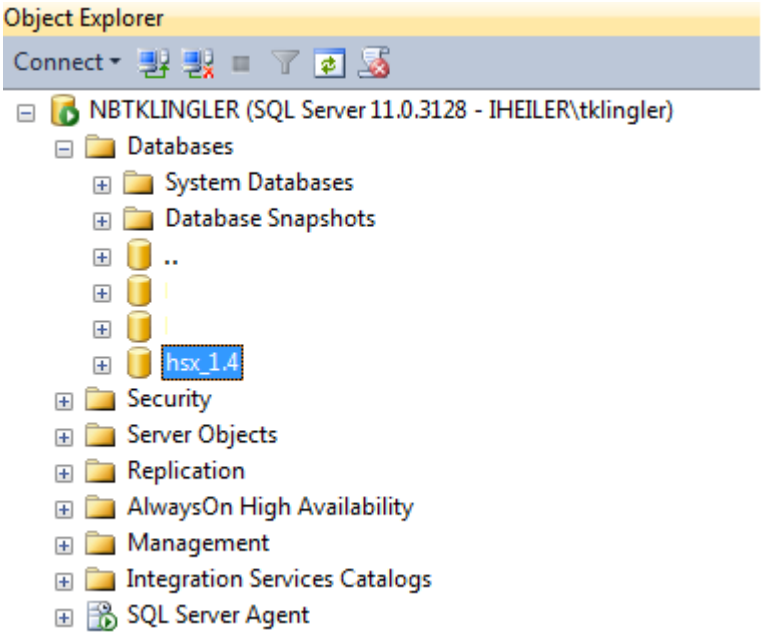
Perform the following steps to finally create the database schema.

1. Open the folder **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/database**
2. Run the **setup.cmd,** while right clicking on the setup.cmd and choosing "run as administrator".
3. A successful console output should look similar to the following screenshot.

Screenshot: Setup.cmd console output



Screenshot: SQL Server Management Studio 2012 showing created database

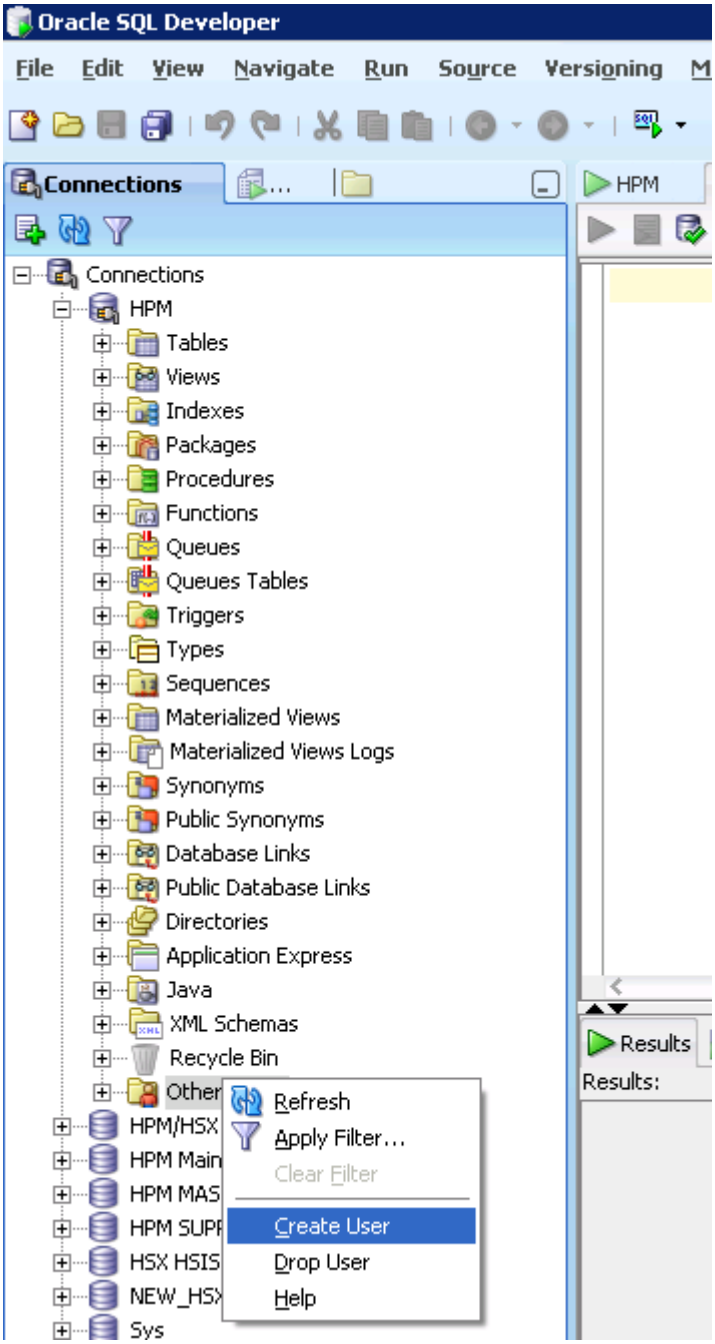


6.5.4 Alternatively: Setup custom database manually

6.5.4.1 Setup Oracle Schema

To create a new user/schema, log in with **Oracle SQL developer** and the **SYSTEM** account. Navigate to "Other users..." and choose "Create User" in the context menu.

Screenshot: Oracle SQL Developer showing how to create an database user.



Enter a user name (which will be the schema name, too) and a corresponding password. This password will be needed later when configuring the jdbc connection.

Choose appropriate tablespaces:

- Default Tablespace: USERS
- Temporary Tablespace: TEMP

On the **System Privileges** tab, grant the following privileges:

- CREATE SEQUENCE

- CREATE SESSION
- CREATE TABLE
- CREATE TRIGGER

On the **Quotas** tab, grant **Unlimited Tablespaces to USERS**.
Click **Apply** to create the user.

If you use a **command-line tool** like **sqlplus** the following script will create the user described above. Change "HENRI" and "heiler" to the name and password of your database.

```
-- USER SQL
CREATE USER HENRI IDENTIFIED BY heiler
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP;
-- ROLES
-- SYSTEM PRIVILEGES
GRANT CREATE SEQUENCE TO HENRI;
GRANT CREATE TABLE TO HENRI;
GRANT CREATE SESSION TO HENRI;
GRANT CREATE TRIGGER TO HENRI;
 -- QUOTAS
ALTER USER HENRI QUOTA UNLIMITED ON USERS;
```

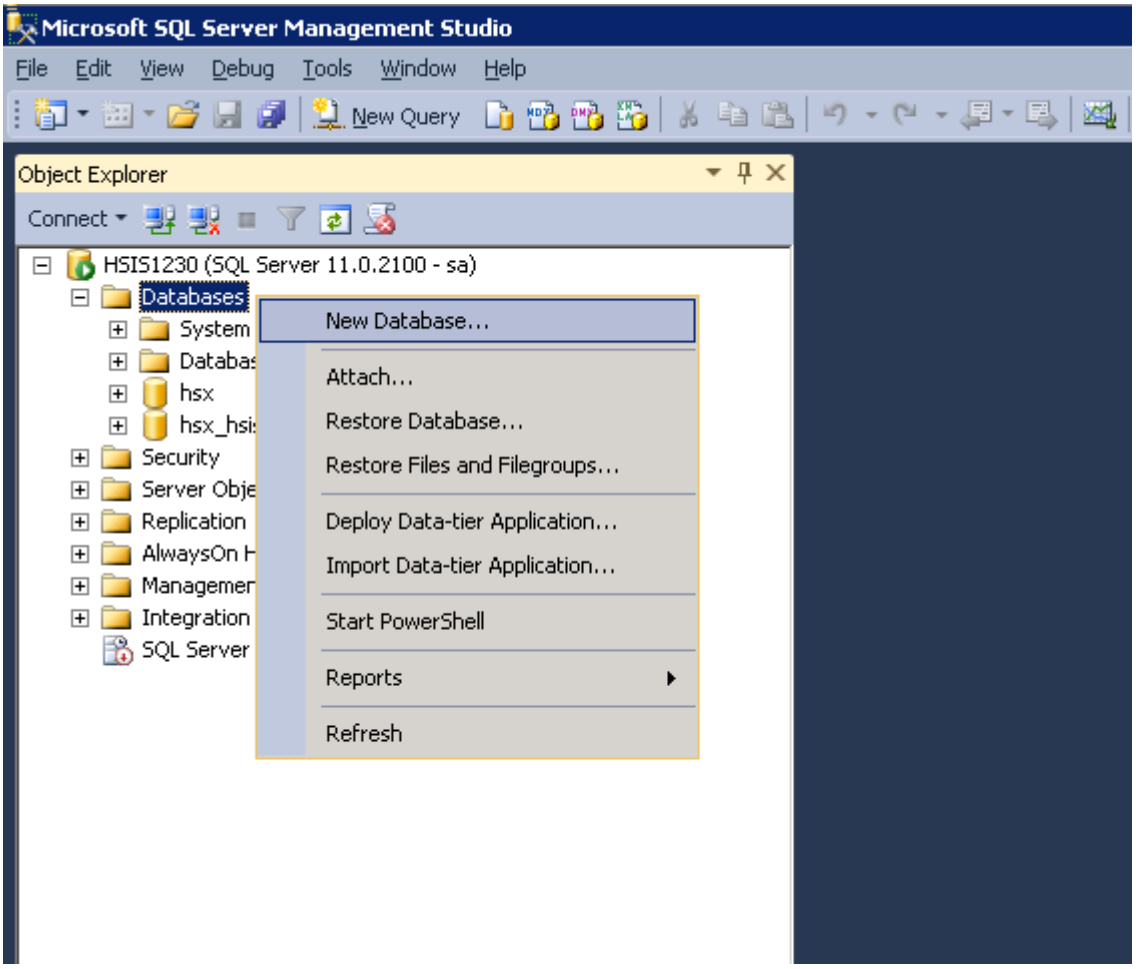
Oracle Password Expiration

By default, the user password expires after a certain period of time. To disable password expiration you will have to execute the following lines:
`alter profile default limit password_life_time unlimited;`

6.5.4.2 Setup MS SQL Schema

To create a new database, start the **SQL Server Management studio** and log in with a user that has either the role **dbcreator** or **sysadmin** assigned. Right click on "Databases" and click on "New Database..." to create a new database.

Screenshot: Microsoft SQL Server Management Studio 2012 showing how to create an database.



Enter a database name, e.g. "HENRI" and select an appropriate owner. This owner and his credentials are needed when configuring the jdbc connection later on. The database **collation** is the same as for the Product 360 Core Database (**Latin1_General_CS_AS**).

Press OK to create the database. Afterwards right click on the new database and choose "New Query" to execute the following script and change the default isolation mode to **READ_COMMITED_SNAPSHOT** (more info):

Change "HENRI" to the name of your database. This statement may take several minutes.

```
alter database HENRI set READ_COMMITTED_SNAPSHOT on with NO_WAIT;
alter database HENRI set ALLOW_SNAPSHOT_ISOLATION on;
```

> The **NO_WAIT** option causes the statement to fail immediately, if there are open connections to the database. If this is the case, make sure that all connections are closed. You can call **sp_who** to list all open connections.

To close all open connections and run the change script for the isolation mode you can execute the following sql script:

```
-- go to single user mode set your current connection to use master otherwise you
might get an error
use master
ALTER DATABASE HENRI SET SINGLE_USER WITH ROLLBACK IMMEDIATE

-- change isolation mode
alter database HENRI set READ_COMMITTED_SNAPSHOT on with NO_WAIT;
alter database HENRI set ALLOW_SNAPSHOT_ISOLATION on;

-- go back to multi user mode
ALTER DATABASE HENRI SET MULTI_USER
```

Verify the isolation mode settings via the following command:

```
select snapshot_isolation_state, snapshot_isolation_state_desc,
is_read_committed_snapshot_on from sys.databases where name = 'HENRI';
```

Result should look similar to this:

	snapshot_isolation_state	snapshot_isolation_state_desc	is_read_committed_snapshot_on
1	1	ON	1

As soon as the script to create the table spaces has been executed successfully there is no need to run any additional database scripts manually in the future.
The server takes care of executing any database updates.

7 Elasticsearch Installation

7.1 Prerequisites for the following products

The Elasticsearch is a prerequisite for Product 360, and has to be installed before it.

Elasticsearch is mandatory for Product 360 production installation

The Audit Trail feature and Fulltext search feature uses Elasticsearch.

7.2 Installing the Elasticsearch 7.x.x

The procedure for setting up the Elasticsearch 7.x.x for Windows is as follows:

- Download the zip from any of the locations listed below
  - https://www.elastic.co/downloads/past-releases/elasticsearch-7-11-0

- Extract the zip file
- Go to *bin* folder and open command prompt
    - run the below command
      bin>elasticsearch
- Server will start and is accessible at below url
  http://localhost:9200/_search

> **Configuration of Elasticsearch**
>
> Elasticsearch can be configured based on customer needs, there are different options available in elasticsearch.yml file. Follow official Elasticsearch setup documentation at https://www.elastic.co/guide/en/elasticsearch/reference/current/setup.html

7.3 Default Elasticsearch Ports

- Ensure you be aware of the database ports your database server is running on.

Port	Database
9200	Elasticsearch

7.4 Installing the Kibana (optional)

Kibana is a free and open user interface that lets us visualize the Elasticsearch data. It also helps in visualizing the metrics.

Follow official Kibana setup documentation at https://www.elastic.co/guide/en/kibana/current/setup.html

7.5 Pre-Installation Checklist

> Elasticsearch server needs to be installed separately.

> *Elasticsearch is a third party application neither developed nor shipped directly by Informatica. Therefore it is recommended to check install and guideline documentation directly on the website of the vendor to follow best practices.*

7.5.1 Version Requirement

Product 360 is compatible with Elasticsearch version 7.x

7.5.2 License Requirement

The Elasticsearch server is available under multiple different licenses.

- Basic (Elastic License) or higher license is recommended

7.5.3 System Requirements

It is recommended that you deploy the Elasticsearch server separately on a single machine or cluster of machines. With the data volume increase, extra nodes should be added to the cluster for better performance.

> It is recommended to install a minimum of 2-node Elasticsearch cluster for a Product 360 production installation.
>
> Refer to official documentation before setting up https://www.elastic.co/guide/en/elasticsearch/reference/7.11/high-availability.html

7.5.3.1 Memory Requirement

The Elasticsearch server needs lot of memory, that is completely allocated at start time ensuring a fast search index build and searches.

- 32 GB is recommended

> Elasticsearch heavily relies on the filesystem cache in order to make search fast. In general, at least half the available memory should go to the filesystem cache.

7.5.3.2 Hardware Requirement

The Elasticsearch server needs fast drives and fast CPU, that is completely allocated at start time ensuring a fast search index build and searches.

- 512 GB SSD is recommended
- 8 CPU cores is recommended

It is recommended to always use local storage, remote filesystems should be avoided.

7.5.4 Security Requirement

It is recommended to enable the security pack provided by Elasticsearch, so that Product 360 can communicate with Elasticsearch over a secured HTTPS connection.

Elasticsearch security

It is recommended to secure the Elasticsearch cluster in all aspects by following the steps from official documentation at https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-security.html

7.5.5 Further Reading

It is recommended to follow the best practices and settings guidance defined in the Elasticsearch website while setting up the Elasticsearch server.

https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html

8 Server Installation

This page describes how the Informatica Product 360 application server. The application server already contains the web and service api interfaces. This documentation is valid for single as well as multi-server installations.

- Prerequisite (see page 81)
  - OS User Permissions (see page 81)
    - Windows (see page 81)
    - Linux (see page 83)
  - OS Volume Shares and Permissions (see page 84)
    - Single Server (see page 84)
    - Multi Server (see page 84)
  - Default Product 360 Server Ports (see page 84)
  - Encryption of secure information (see page 85)
    - Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information (see page 86)
  - Large memory pages under Linux (see page 86)
- Application Server (see page 86)
  - Download and Extract Binaries (see page 87)
  - Configuration (see page 87)
    - General Server Settings (server.properties) (see page 88)
    - Startup parameters (_environment.conf) (see page 89)

- NetworkConfig (see page 90)
- License (see page 92)
- Service Installation (see page 93)
  - Windows (see page 93)
  - Linux (see page 94)
- Media Asset Provider (see page 94)
  - Media Manager Provider (see page 94)
  - Classic Provider (see page 94)

8.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Product 360 Core Database (see page 35)
  The Server Database manual describes how to initially setup or update the Product 360 server database schemas for a new release.

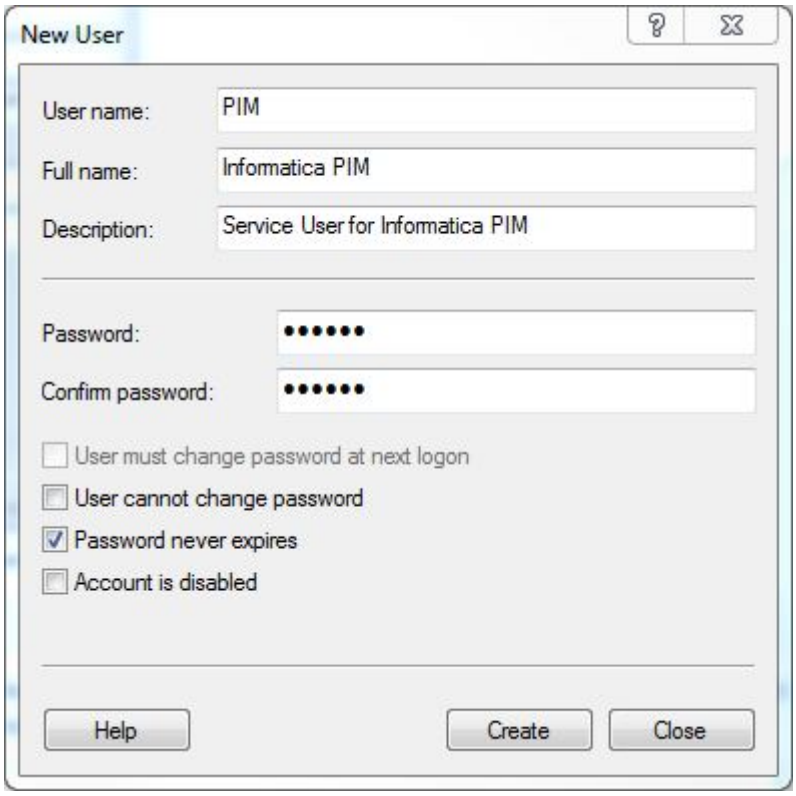
8.1.1 OS User Permissions

8.1.1.1 Windows

The user who installs the MDM Product 360 needs to have local administrative permissions.

Create Service User

- Open Start > All Programs > Administrative Tools > Computer Management > Local Users and Groups > Users > New User ...

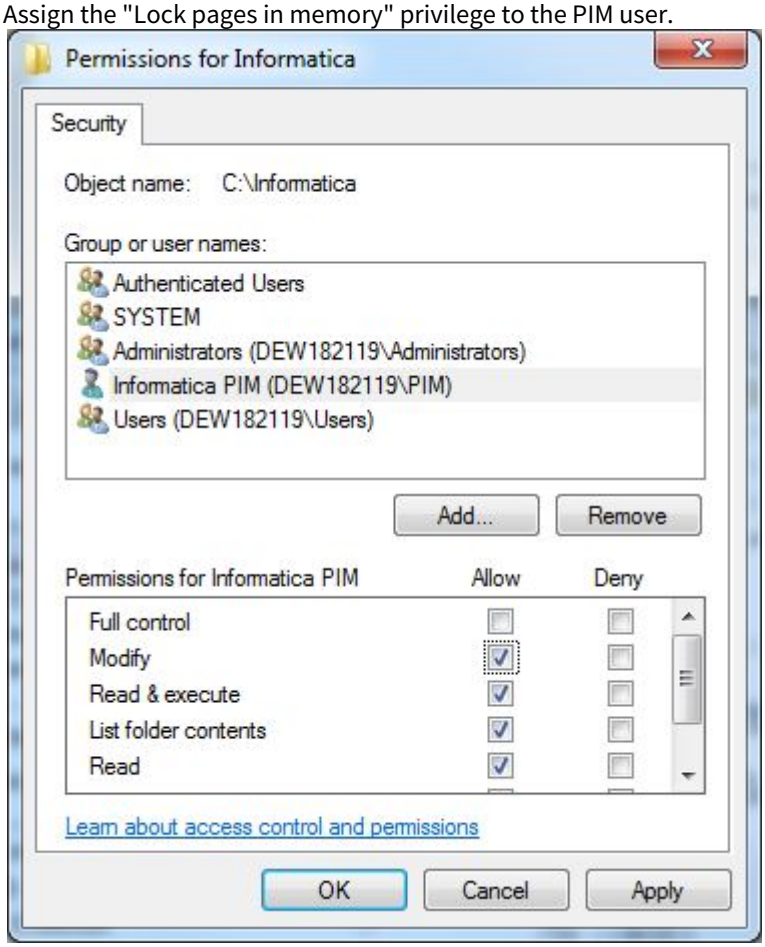


- Create a new user account for the service (e.g. PIM).

> In case the host machines are part of a domain, we recommend using a special domain user for the following steps, rather than creating you're own local user.
> Please contact your network administration department so they create this service user for you.

- Open Start > All Programs > Administrative Tools > Local Security Policy > Local Policies > User Rights Assignment.

Assign the "Lock pages in memory" privilege to the PIM user.



8.1.1.2 Linux

The user who installs the MDM Product 360 needs to have the right to install services.

The user running the MDM Product 360 server needs a valid locale. Please check with the following command if a locale is set for your user:
`http://man7.org/linux/man-pages/man1/locale.1.html#EXAMPLE`

```
locale
```

If no valid locale is set then you can set it with the following command.

```
export LANG = en_us.utf-8
```

An invalid locale can lead to a server crash when executing data quality rules.

Create Service User

To create a new user account for the service (e.g. PIM), use either the graphical tool of your distribution or a command line tool like `adduser`.

The user needs to have the right to start a service otherwise it is not possible to start the application server

8.1.2 OS Volume Shares and Permissions

8.1.2.1 Single Server

For single server installations no shares or special permissions must (and should) be created. The only important thing is that the user which is used to run the Product 360 Server service must have full permissions to the folder

which is defined in the `filestorage.dir.shared` property of the `server.properties` file.

8.1.2.2 Multi Server

In order to prevent any kind of "single point of failure" in the multi-server deployment, it must be guaranteed that all servers have equal access to the same file storage. This can either be achieved by using SAN technology
so that all servers would have *the same* virtual local drive. In this case, no shares need to be configured. This approach is especially recommended for productive clusters.

Development and test environments can also be configured to use a simple `SMB` share. In this case the Product 360 service user must have full `read` and `write` permissions to this share (other users do not need to have access to it!)

8.1.3 Default Product 360 Server Ports

> ⚠ If possible, use the default ports for the installation, only change the ports if they are already bound by another application in your company.

Port	Protocol	Product 360 Module
1712	tcp	Desktop connection. This port is used to connect the Desktop Client and Server. The used protocol is an internal low-level protocol, optimized for high performance throughput.

Port	Protocol	Product 360 Module
1512	http	Web Server Port (Jetty) which is used for the Web Client as well as the Service API or file transfer. The used protocol is HTTP (or REST via HTTP)
1812	tcp	Data Grid communication. Needed for the synchronization heartbeat of the cluster. For data synchronization the Hazelcast framework is used. Hazelcast itself uses a dynamic range of outgoing ports determined by the OS for communication between nodes. These outgoing ports strategy can be changed via the property <outbound-ports> in the deployed hazelcast.xml config file. See chapter "Server configuration - Hazelcast configuration (hazelcast.xml)" how to configure Hazelcast.
55555	tcp	Default Java Management Extensions Port which is needed to attach troubleshooting and tuning tools. For security reasons this port must not be reachable from outside the server machine.
61616	tcp	The port for the message queue connection.
25	smtp	Product 360 Server is capable to send e-mails in various functional areas, for this it needs access to a smtp e-mail server
445 and 139	smb and tcp	Windows file share ports for the media asset file communication when used with the Product 360 Media Manager module

8.1.4 Encryption of secure information

Product 360 supports the encryption of secure information like passwords in configuration files. The encryption will be executed only if your secure information in the configuration files is enclosed by the

marker `[_to_encrypt_]`.
So, if you want to have e.g., the password "MyPassword" encrypted in a configuration file just use the marker before and after the password like this: `[_to_encrypt_]MyPassword[_to_encrypt_]`.

For example:

properties file

```
# INFA BPM
infa.bpm.base.url       = <ENTER THE INFA BPM BASE URL HERE>
infa.bpm.workflows.path = services/REST
infa.bpm.user           = <ENTER THE AUTHENTICATION USER HERE>
infa.bpm.password       = [_to_encrypt_]MyPassword[_to_encrypt_]
```

xml configuration file

```
<network>
    <node identifier="audit-server" host="localhost" port="2801" username="Administra
tor" password="[_to_encrypt_]MyPassword[_to_encrypt_]"/>
</network>
```

8.1.4.1 Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information

Product 360 provides a default implementation for the encryption of secure information with an internal and securely stored Key using AES-256.
For sophisticated deployments we recommend integrating with Encryption Key Management solutions like Amazon AWS or Azure KeyVault and use the API we offer to send and receive data for encryption to these key stores securely

8.1.5 Large memory pages under Linux

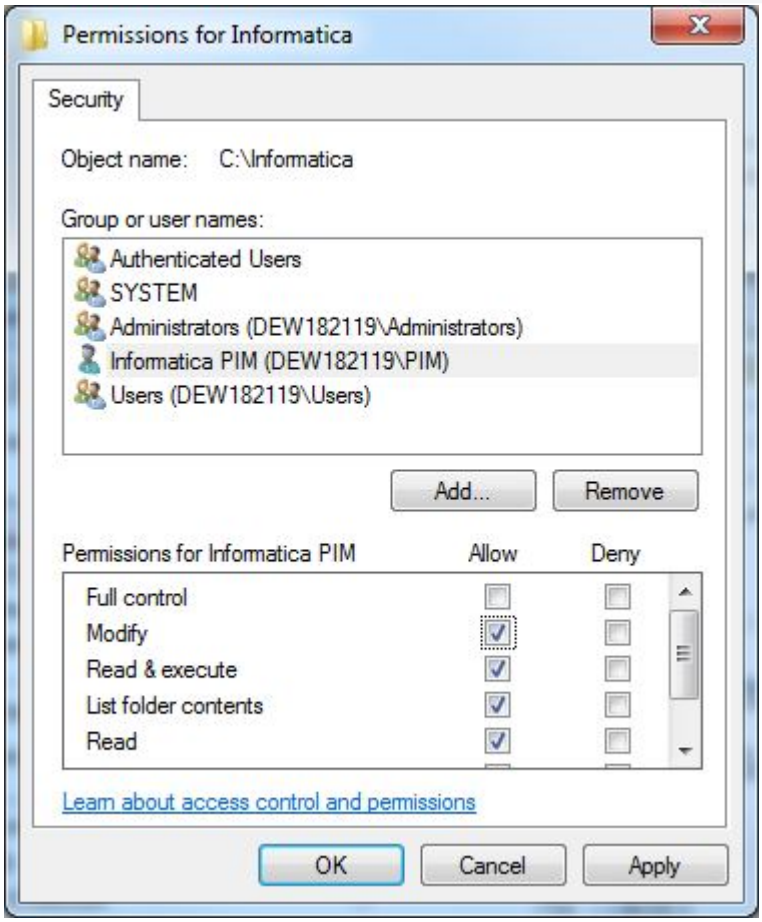
In order to use large memory pages (which is enabled by default, see JVM parameter `XX:+UseLargePages` in `wrapper.conf`), you may have to change the operating system configuration as described in the following article:
https://www.oracle.com/technetwork/java/javase/tech/largememory-jsp-137182.html

8.2 Application Server

The installation is identical on all servers of the cluster with the exception of the `_environment.conf` file which holds the individual server's identifier in case of a cluster installation

8.2.1 Download and Extract Binaries

- The package name is `PIM_<version>_<revisionNumber>_server_win64.zip` resp. `PIM_<version>_<revisionNumber>_server_linux64.tgz.`
- Extract the package into a directory, e.g. `C:\Informatica\PIM` (= `<PIM ROOT>`).
  The directory structure should look like this: **`<PIM ROOT>\server`** and **not** like this `<PIM ROOT>\PIM_<version>_<revisionNumber>_server_win64/server`
- Make sure that the PIM service user has full permissions on the `<PIM ROOT>` and all children.



8.2.2 Configuration

We will only touch the minimally needed properties for the installation in this section, please find a detailed description of all properties in all configuration files on the Server Configuration page.

> ⚠ If you want to encrypt the passwords used in the configuration files, please refer to chapter Encryption of secure information (see page 85) in the Server Installation manual. The passwords marked as to encrypt will be encrypted if you save the configuration file or before the distribution of configuration take place.

> If you want to connect the P360 Server to an Oracle Database via TCPS, please refer to chapter "How to configure a secure database connection for Product 360 Server" in the "Server Configuration" manual.

8.2.2.1 General Server Settings (`server.properties`)

File: `<PIM ROOT>\server\configuration\HPM\server.properties`

The following properties needs to be adjusted at least. In case of an integration with Informatica MDM or Informatica BPM you will need to adjust additional properties in this file. Please see the corresponding documentation for this.

Property	Description
File Transfer Settings Is is crucial for multi-server deployments that *all servers* can access the *same file storage* and the *same directories* in there. For example, it might be that Server A uploads files to the import area in the file storage, but Server B is executing the import for this. So, Server B needs to have the identical file access then Server A. The currently available default implementation for the file storage is SMB which uses the SMB protocol to access the files. Please note that the file transfer from the Desktop Client is done using HTTP only. **Clients do not need to have access to the file transfer shares, only the servers!**	
`filestorage.dir.shared`	Folder which has to be accessible by each Product 360 server. In case of a single server system, the folder does not have to be a shared one. In case of multi-server, you might want to use a common file store with an SMB share or some kind of Network storage on which every server node has access.
Customer license key	
`license.customer.file.local`	Local path to the license file. Please contact the Informatica Product 360 Partner Management to obtain a license file.
`license.customer.key`	Appropriate customer key (in case of multiline keys, use backslash at the end of the line)

Property	Description
Repository Settings	
`repository.default.language`	The default language of the repository regarding all language specific aspects like e.g., default logical key language. Possible values: Key synonyms of the corresponding language entries defined in the repository enumeration "`Enum.Language`", e.g. `"de"` or `"en_US"` - default is German, if property does not exist. **Note:** The repository language **MUST NOT** be changed as soon as entity data such as items/products/variants or structures/structure groups have been created and exist in the database. In such a situation, the stability of the system can no longer be guaranteed since logical key fields most likely will contain null values.
Database settings for Microsoft SQL Server and Oracle **Please visit the corresponding database setup settings in the chapter "Provide database connection settings" of the page "Server Database" which are also for server installation.**	

8.2.2.2 Startup parameters (`_environment.conf`)

File: `<Product 360 ROOT>\server\configuration\HPM\_environment.conf`

Parameter	Description	Default/Example
`MEM_MAX`	Change this parameter to the maximum heap space for the Java VM. Never configure more than the physically available memory of the machine. (The normal rule is: Physical memory - 1 GB for the OS = maximum heap space.)	e.g., 16384M for 16 GB Heap Space
`NAME_SHORT`	Defines the service name / console window title	Product_360_10.5

Parameter	Description	Default/Example
`NAME_LONG`	For visualization in the services overview	Informatica MDM - Product 360 v10.5
`JMX_PORT`	Defines the port for the java management extensions (JMX)	55555
`SERVER_IDENTIFIER`	Defines the identifier of the server. The identifier must match to the network node identifier of the NetworkConfig.xml file (see below).	pim-server1

8.2.2.3 NetworkConfig

Open the file `<PIM ROOT>\server\configuration\HPM\NetworkConfig.xml` in an editor and adjust the mandatory properties. Add node elements for each node in the cluster.
See the Server Configuration for details on all properties you can adjust in this file. For ease of the installation, we only have a subset of the available settings here.

It is important to note that the network configuration file is identical on all nodes of a cluster. Only the `SERVER_IDENTIFIER` in the `_environment.conf` file determines which of those servers the current node is. This way the configuration for the servers can be more or less identical and can just be copied to all the nodes of the cluster (aside from the _environment.conf file of course)

Ports must be open!

All communication ports which are defined in the NetworkConfig.xml must be open for all servers in the cluster. Especially the `data-grid` as well as the `hlr-tcp` port. In case the servers can't reach each other, they will not throw an error as they will just assume to be the first one in the cluster to be started. You might not even immediately recognize that the servers do not work as a real cluster together. In case you want to check if the servers are really connected as a cluster, you can check the log file of the second server during startup. Every server which starts up will try to connect to the other servers which are already running, if successful he will log that.

This is a typical log of the first server which starts:

```
INFO   | jvm 1    | 2021/12/10 12:19:22 | 12:19:22,114 INFO
[ServerInitializer 2] [ClusterService] [Myserver1]:1802 [P360] [3.12.1]
INFO   | jvm 1    | 2021/12/10 12:19:22 |
INFO   | jvm 1    | 2021/12/10 12:19:22 | Members {size:1, ver:1} [
```

```
INFO   | jvm 1    | 2021/12/10 12:19:22 | Member [Myserver1]:1802 - c82f2563-
d8e4-40da-9830-1ef53bf8ed3a this
INFO   | jvm 1    | 2021/12/10 12:19:22 | ]
```

All subsequent servers should have the already started servers in the member's array.

Element/Attribute	Description	Example/Default
`network`	Root element of the network configuration, contains one or more nodes	
`node`	**Represents a server node in the cluster**	
`identifier`	Unique identifier of the node within the network. See *-Dppm.nodeIdentifier* command line argument below!	`product360-server1`
`host`	The host name / IP address this node runs on. Note: Do not use localhost or similar addresses. The host name or IP address in this attribute must be visible from all nodes in the cluster. In case the server has the CLIENTS_SERVER role, it also must be visible from the desktop clients. **Please use only CAPITAL LETTERS for the host name**	
`default-role` mandatory attribute	Default role(s) each server node must have at start time. Available roles are `CLIENTS_SERVER`, `JOB_SERVER`, `MQ_CONSUMER_SERVER`, `PRIORITY_JOB_SERVER`. The server roles can not be modified during runtime of the server.	`CLIENTS_SERVER`. `JOB_SERVER`, `MQ_CONSUMER_SERVER`, `PRIORITY_JOB_SERVER`
`node/web`	**Web relevant protocol settings (either `HTTP` or `HTTPS`)**	

`useHttps`	Enables/disables the SSL protocol. Default is false - in case you want to enable it, you need to provide a valid SSL certificate and use the https element. See Server Configuration for details	`false`
`node/web/http`	`HTTP` **specific settings**	
`port`	`HTTP` port to be used for the web server	1512
`node/data-grid`	**Settings for the distributed data grid**	
`port`	Port to be used for the data grid connection.	1812
`node/internal/hlr-tcp`	**Settings for the internal communication protocol**	
`port`	Port for incoming / outgoing connections regarding internal communication	`1712`
`node/snmp`	**Settings for the SNMP protocol communication**	

`oid`	Object id of the node in the cluster. Each node must have a unique oid.	`1.1 (first node)`
		`1.2 (second node)`
		`and so on...`

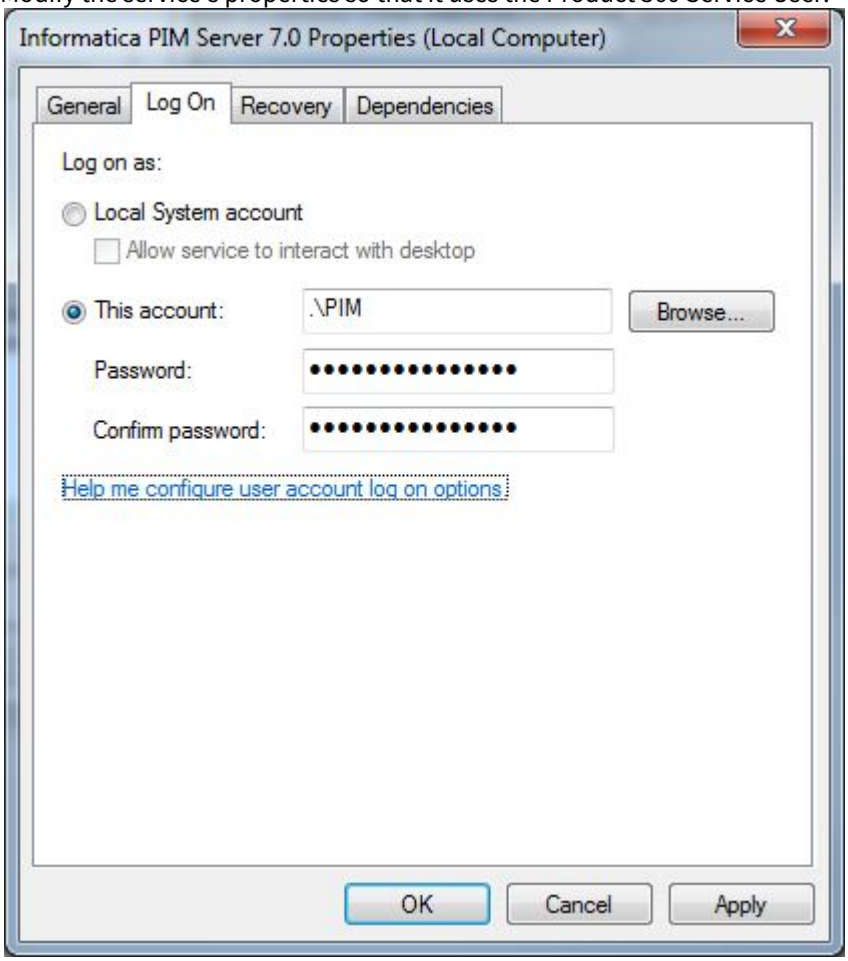
8.2.3 License

- Create a new folder underneath the file storage root folder which has been provided by the `filestorage.dir.shared` property called `license`.
- Copy the license file to this folder.

8.2.4 Service Installation

8.2.4.1 Windows

- Install the service manually by executing
  `<PIM ROOT>\server\install.cmd` (Windows) resp. `sudo <PIM ROOT>/server/install.sh` (Linux)
  Linux: If the Product 360 server should not run as root, the user can be specified in `<PIM ROOT>/server/service/pimserver.sh` and change the line
  `#RUN_AS_USER=`
  to
  `RUN_AS_USER=<USERNAME>`
  whereby `<USERNAME>` is the name of the Product 360 Service User
- Open Start > All Programs > Administrative Tools > Services
- Modify the service's properties so that it uses the Product 360 Service User.



- Make sure that the startup type is "Automatic"
- Start the service

> Since the application server needs to have full access to the file share, it is necessary to also adjust the windows service of the application server to use the service user we defined and make sure that this user has full access on the file share.

8.2.4.2 Linux

- Install the service manually by executing
  `sudo <PIM ROOT>/server/install.sh`
  Linux: If the Product 360 server should not run as root, the user can be specified in `<PIM ROOT>/server/service/pimserver.sh` and change the line
  `#RUN_AS_USER=`
  to
  `RUN_AS_USER=<USERNAME>`
  whereby `<USERNAME>` is the name of the Product 360 Service User
- Start the service Informatica Product 360 by starting the service via
  `service Product_360_10.5 start`

8.3 Media Asset Provider

In order to work with multimedia documents such as images, videos and documents the Product 360 application server needs a media asset provider. If not configured otherwise, it is pre-configured with it's build-in provider (aka Classic Provider, HLR). The build-in provider is merely a simple directory based storage for multimedia documents with limited capabilities regarding image processing etc. Informatica recommends to always use the Media Manager module since it provides a richer set of functionalities.

8.3.1 Media Manager Provider

Please see separate instruction for the Media Manager Integration (see page 129)

8.3.2 Classic Provider

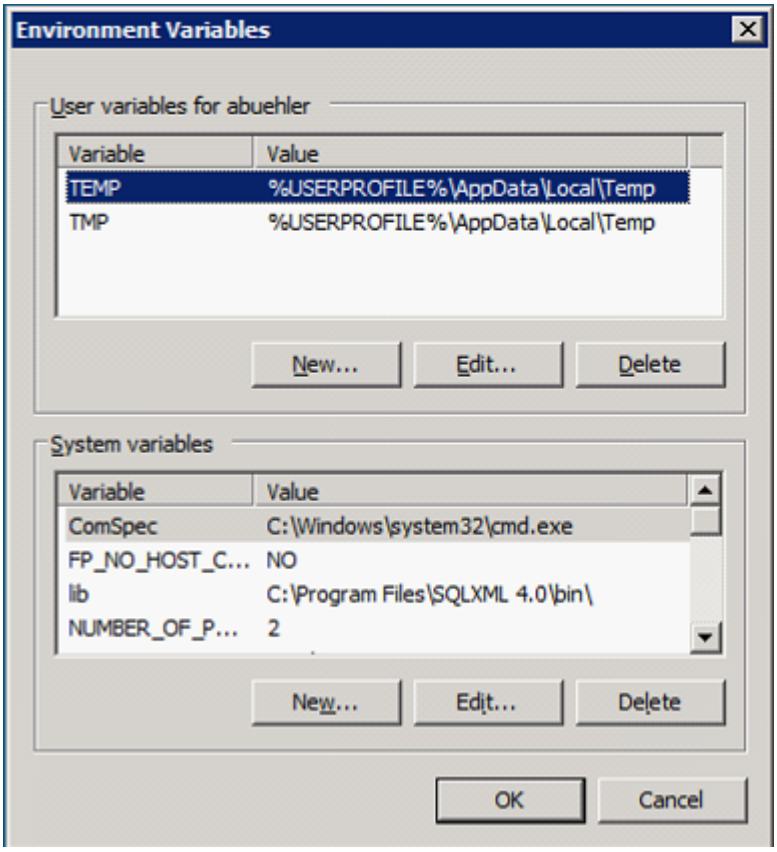
> The Classic Provider is only supported for Windows operating system!

8.3.2.1 GraphicsMagick for Classic Provider

The Classic Provider uses GraphicsMagick for processing preview images. This 3rd party tool which is located on the 3rd party archive cd must be installed separately. Classic Provider works with Version GraphicsMagick 1.3.14-Q16 (32 bit for Windows) (other Versions are not tested and are not recommended to be used!). You can find the needed version (`GraphicsMagick-1.3.14-Q16(32 bit for windows)`)

on the 3rd party archive cd, **install it according to it's own installation** instructions. See the Configuration Manual for more information about all possible configuration parameters.

GraphicsMagick uses the TEMP and TMP environment variables to work with temporary files. Unfortunately it does not support whitespaces in the paths to those temporary folders. Therefore you need to adjust the TEMP and TMP variables to have no whitespaces in them (take care about the `%USERPROFILE%` variable - it might contain whitespaces!).



9 Desktop Client Installation

This pages describes the installation of the Informatica Product 360 Desktop Client

- Prerequisite (see page 96)
- Binaries (see page 96)
- Installing the client with MSI file (see page 96)
- Starting the client (see page 99)
- Single Sign-On (see page 101)
  - LDAP Authentication (see page 101)
  - SAML Authentication (see page 102)

9.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Server Installation

9.2 Binaries

To obtain the Product 360 download package please raise a Shipping Request with Informatica.

The client archive is distributed within the Product 360 core archive and has the following format `PIM_<Version>_<Revision>_client_win64.msi`

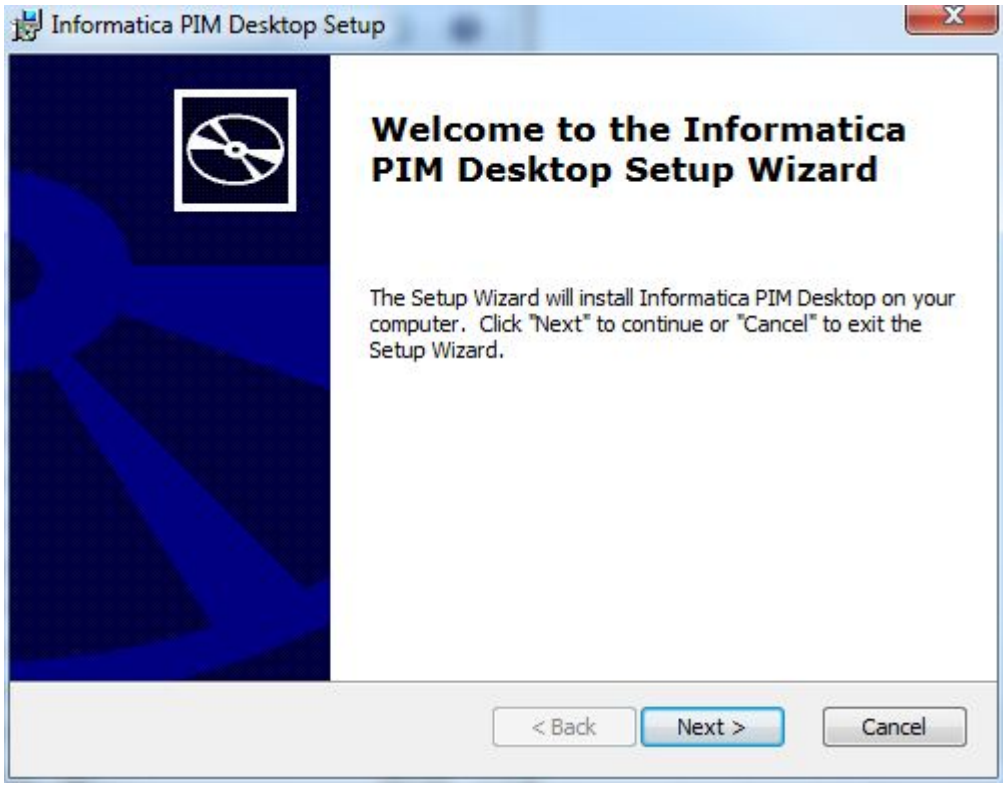
9.3 Installing the client with MSI file

This chapter describes how to install the client by means of a MSI file which is a Microsoft Installer executable providing a wizard like installation procedure.

Perform the following steps:

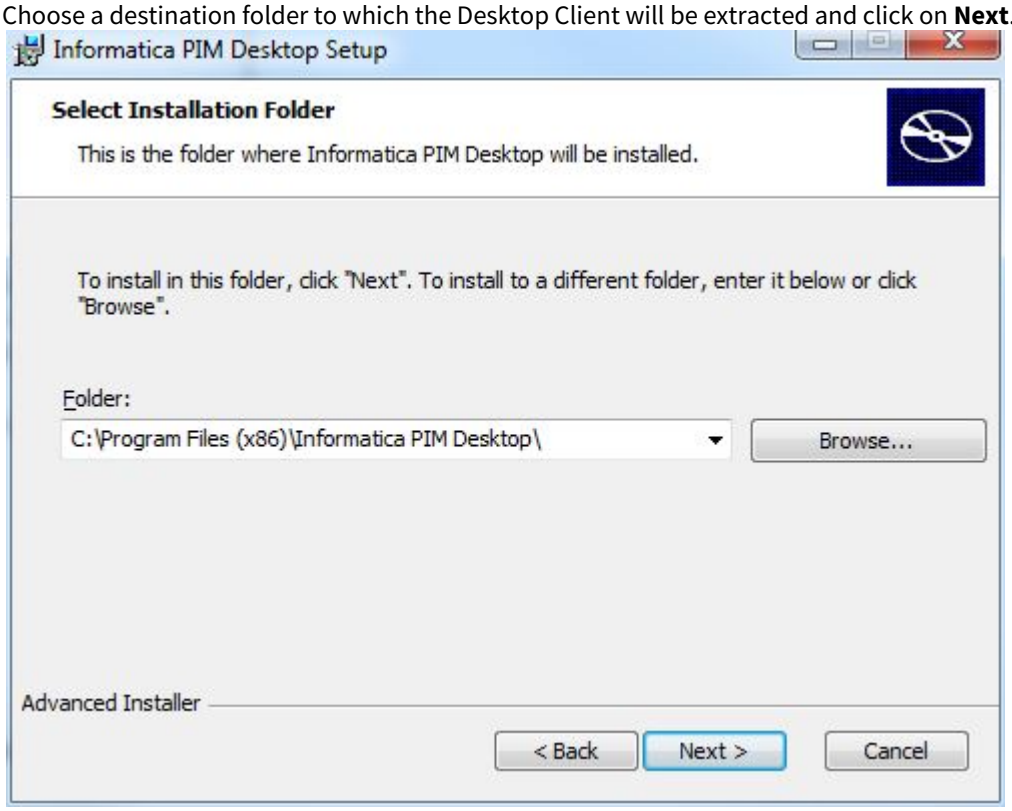
1. Execute the installer file `PIM_<Version>_<Revision>_client_win64.msi (` e.g. `PIM_8.0.00.00_Rev-4711_client_win64.msi)`.

2. Click on **Next**.



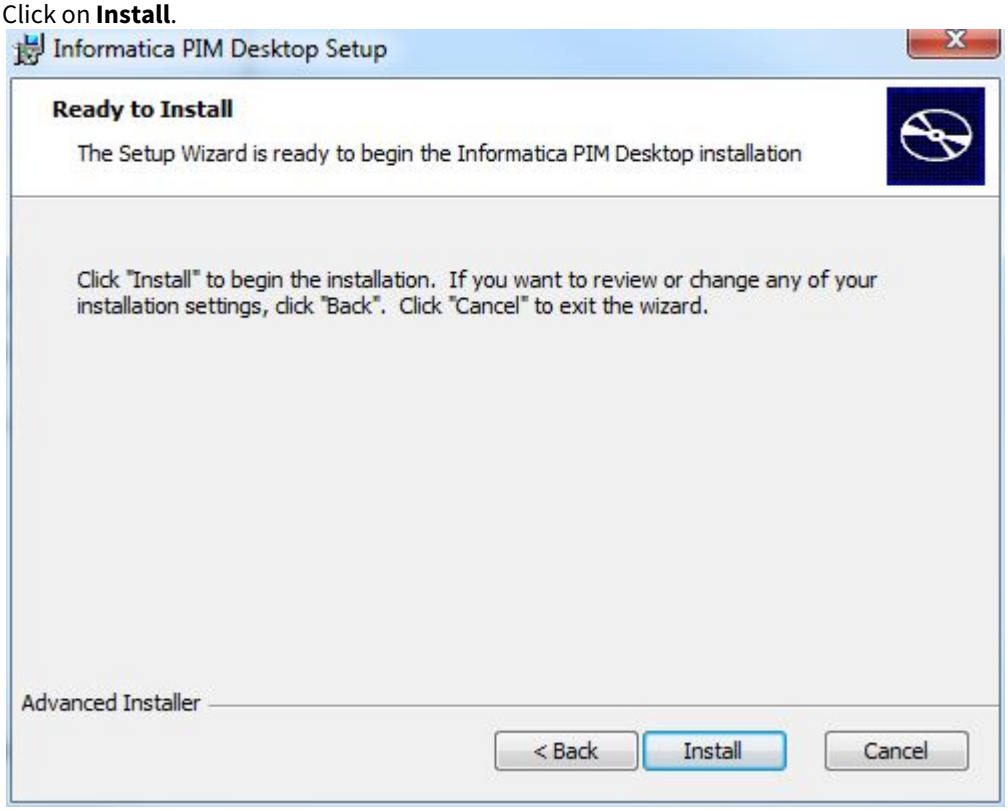
Welcome screen of Informatica Product 360 - Desktop Setup Wizard

3. Choose a destination folder to which the Desktop Client will be extracted and click on **Next**.



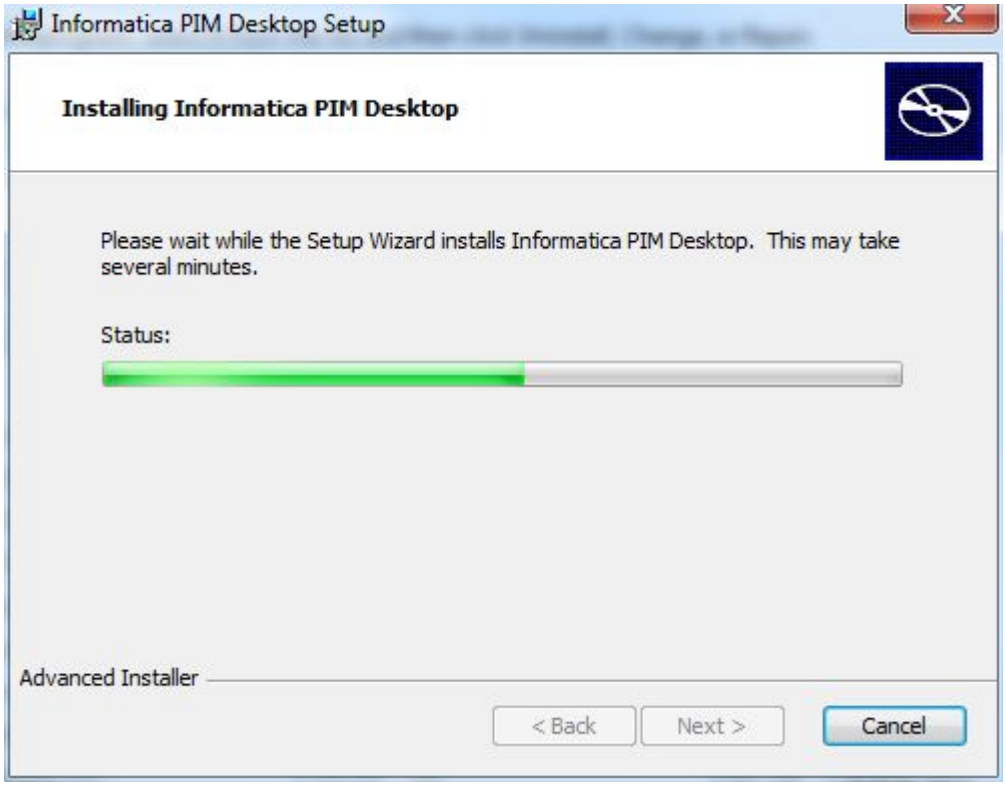
Selecting the installation folder

4. Click on **Install**.



`Starting the client installation`

The Desktop Client will be extracted to the destination directory.



Installation progress screen

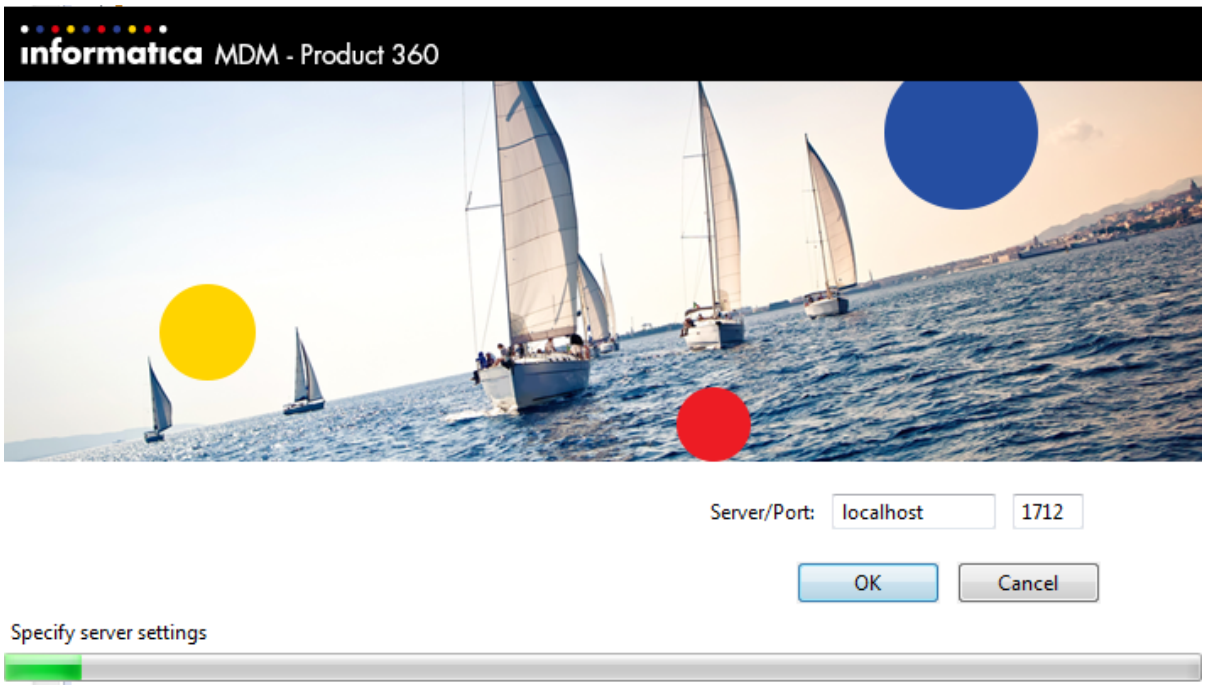
5. Confirm the signature warning dialog (only Windows Vista and Windows 7).
6. Click on **Finish** to exit the Setup Wizard.

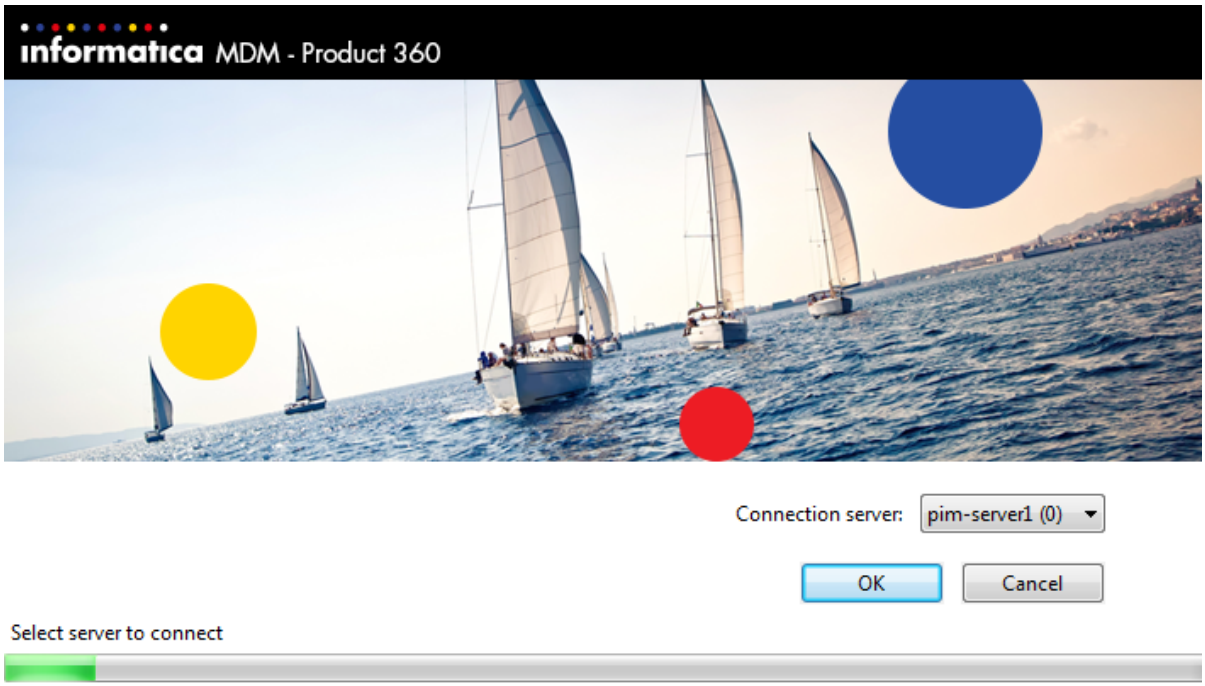
> In case you have a customized client, you might not have the MSI installation package, but the zipped archive `PIM_<Version>_<Revision>_client_<ARCH>.zip`. The client's installation is really nothing more then unpacking the zip file to a folder of your choice in which you have modify permissions. Deinstallation is done by deleting the directory in which you unzipped the client.

9.4 Starting the client

Perform the following steps:

- Run the Desktop Client by double clicking the "Informatica Product 360 Desktop" shortcut on your desktop or in your start menu.
- While starting, the Desktop client tries to use the connection info from the ServerConnection.xml file in order to connect to the initial client server. Given that there are more than one "client servers" available in the server cluster, the initial server then automatically delegates the connection to the server with the least number of connected clients, to the so-called dialog server. When pressing and holding Ctrl during client start, the connection info to the initial server can be specified manually (as usual).

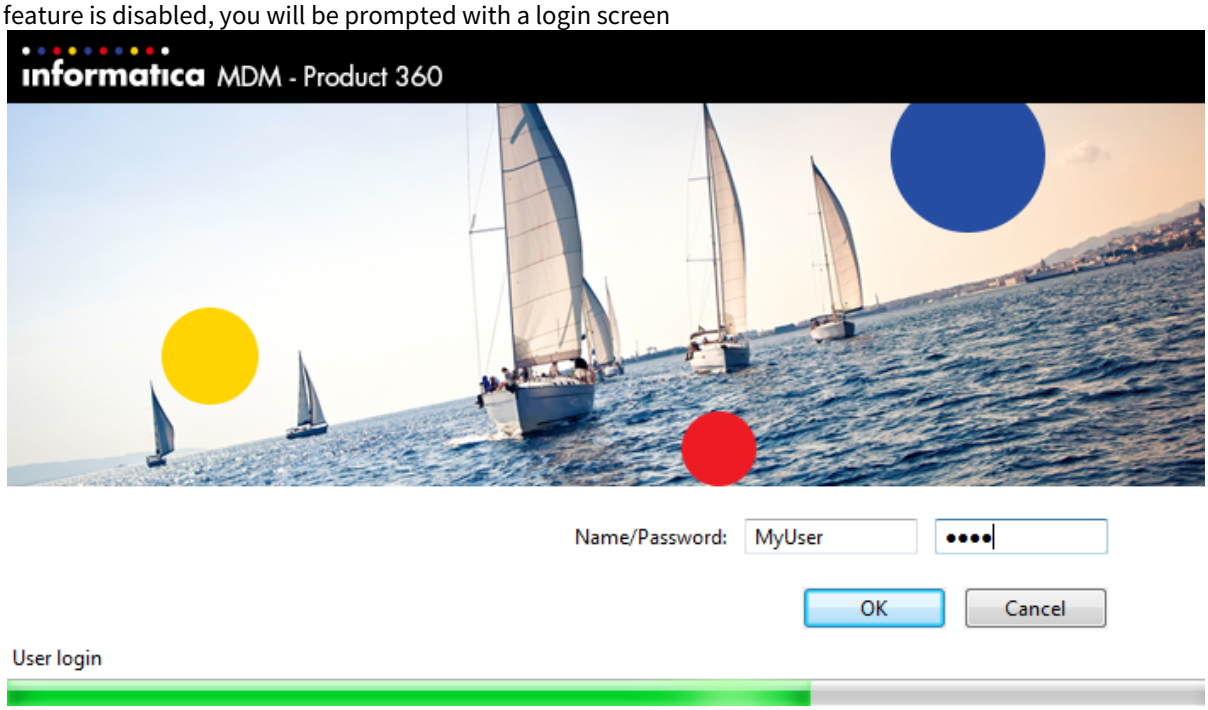


- Afterwards, the dialog server can be selected manually from a drop down box, which contains a sorted list of all available client servers including the number of already connected Product 360 Desktop clients. In case the client cannot find the server with the default connection settings, it will prompt for alternative connection settings.
- 

- When the client was able to connect to a server, he retrieves all information of all the configured servers of the cluster. Next time if a server is down, the client is able to request the other servers for a connection.

Enter connection settings

- Enter the server name and port of the application server and click OK.
- In case your local windows user is not (yet) known to **Informatica Product 360**, or the Single-Sign-On feature is disabled, you will be prompted with a login screen



Login screen

- Enter your user name and password here and confirm with OK. In case Informatica Product 360 has been started the first time and no user or user group configuration exists yet, you can use the default Administrator account
  Username: Administrator
  Password: Administrator

> If you don't want to use the default connection settings or you want to login as another user than the local windows user,
> you can change the server connection settings and the user login when you keep the `CTRL` key pressed during startup.

9.5 Single Sign-On

9.5.1 LDAP Authentication

In case Informatica MDM product 360 is configured to use LDAP authentication special rules may apply during login.

In case the system is configured to use a single domain from the LDAP server, the users can login just with their user name, otherwise should specify the domain during the login. E.g. myCompany.com\MyUserName or MyUserName@MyCompany.com.

The single-sign on feature is only available on the Desktop Client. It uses the currently logged in Windows user and tries to authenticate this one against the server. If the user can be found, and validated against LDAP the user is automatically signed in.

Depending on the user group configuration in your system, it is possible that the user is instantly created and mapped to the Product 360 user groups based on his LDAP group membership. This works for LDAP authentication as well as single-sign-on.

9.5.2 SAML Authentication

Starting with 8.0.03 it is possible to login to the desktop client via SAML. A detailed description how to configure and activate SAML Single Sign-On is described in the Server configuration section 'SAML Configuration'.

When SAML is enabled in the SamlConfig.xml, the Rich Client will display the login form or login prompt configured by the IdP. No special configuration is required for this scenario.
The SAML login can be skipped by pressing <ctrl> key during client startup process.

The Rich Client Single Sign On also triggers, if configured, the automated user creation, if a default user group is configured.

Possible problems and workarounds that may occur, especially certificate trusts, are described under 'Workaround to prevent the "Invalid Certificate" error (Mozilla)' in the section 'Desktop Operation'.

10 Message Queue Installation

10.1 Prerequisites for the following products

The Product 360 MessageQueue is a prerequisite for Product 360, and has to be installed before it. Additionally the P360 MessageQueue is used for the following products:

- Product 360 - Media Manager

10.2 Installing the Apache Message Queue 5.x.x

The procedure for setting up the Apache Message Queue 5.x.x for Windows is as follows:

1. Uncompress **PIM_<Version>_ThirdPartySoftware.zip** from your Product 360 8.0 distribution to your local computer
2. Navigate to the directory **\ActiveMQ 5.x.x**.
3. Unpack the file **MessageQueue*.zip** to **C:**. (or any other folder)
4. Run Command Prompt as Administrator, navigate to **C:\MessageQueue** and launch the application using the script **startup64.bat**.

5. To manage the Message Queue use the following link: **http://localhost:8161/admin/** and type in admin for user and password.
6. For checking the entries use the following link: **http://localhost:8161/admin/queues.jsp**

To change the connection URL open **C:\MessageQueue\conf\activemq.xml** and modify this entry:

```
<transportConnectors>
      <transportConnector name="openwire" uri="tcp://localhost:61616"/>
</transportConnectors>
```

To change the password for admin open and modify the entry 'admin: admin, admin'

To change the password for admin open **C:\MessageQueue\conf\jetty-realm.properties** and modify the entry 'admin: admin, admin' formatting as 'username: password, role'.

To disable this webconsole open **C:\MessageQueue\conf\activemq.xml** and comment the import of the file jetty.xml:

```
original:
<import resource="jetty.xml"/>

disabled:
<!--
<import resource="jetty.xml"/>
-->
```

10.3 Run Apache Message Queue 5.x.x as a service

1. Run **cmd** as Administrator, navigate to **C:\MessageQueue\activemq\bin\win32** and execute **InstallService.bat**
2. Open the Microsoft service administration.
3. Open the properties of the "Informatica Product 360 ActiveMQ" service.
4. On the "General" tab set the startup type to "Automatic".
5. Click on **OK**.
6. Start the service.

With UninstallService.bat the service can be deleted.

10.4 Enable the JMX for Apache Message Queue

As the Product 360 with JMX can be enabled by How to enable Java Management Extensions (JMX), the JMX can be also enabled for ActiveMQ to observe and manage the performance.

1. Open the **C:\MessageQueue\activemq\bin\win64**\wrapper.conf to enable remote JMX

```
# Uncomment to enable remote jmx
wrapper.java.additional.10=-Dcom.sun.management.jmxremote.port=1616
wrapper.java.additional.11=-Dcom.sun.management.jmxremote.authenticate=false
wrapper.java.additional.12=-Dcom.sun.management.jmxremote.ssl=false
```

2. Restart the Active MQ server
3. Connect JMX tool with Active MQ server: start up **JConsole** or **Java VisualVM** to set the corresponding parameter(e.g. `localhost:1616`) for the host, optionally add some display name for the connection.

10.5 Security (optional)

You can use SimpleAuthenticationPlugin. With this plugin you can define users and groups directly in the broker's XML configuration (conf/activemq.xml by default). Take a look at the following snippet for example:

SimpleAuthenticationConfiguration

```
<plugins>
        <!-- Configure authentication; Username, passwords and groups -->
        <simpleAuthenticationPlugin>
            <users>
                <authenticationUser username="system" password="${activemq.password}"
                    groups="users,admins"/>
                <authenticationUser username="user" password="${guest.password}"
                    groups="users"/>
                <authenticationUser username="guest" password="${guest.password}"
 groups="guests"/>
            </users>
        </simpleAuthenticationPlugin>

      <!--  Lets configure a destination based authorization mechanism -->
      <authorizationPlugin>
        <map>
          <authorizationMap>
            <authorizationEntries>
              <authorizationEntry queue=">" read="admins" write="admins" admin="admin
s" />
              <authorizationEntry queue="USERS.>" read="users" write="users" admin="u
sers" />
              <authorizationEntry queue="GUEST.>" read="guests" write="guests,users"
 admin="guests,users" />

              <authorizationEntry queue="TEST.Q" read="guests" write="guests" />

              <authorizationEntry topic=">" read="admins" write="admins" admin="admin
s" />
```

```
              <authorizationEntry topic="USERS.>" read="users" write="users" admin="u
sers" />
              <authorizationEntry topic="GUEST.>" read="guests" write="guests,users"
 admin="guests,users" />

              <authorizationEntry topic="ActiveMQ.Advisory.>" read="guests,users"
 write="guests,users" admin="guests,users"/>
           </authorizationEntries>
         </authorizationMap>
       </map>
     </authorizationPlugin>
   </plugins>
```

10.5.1 Use SSL over TCP

1. Add the following entry in the activemq.xml, adjust the port depending on your need

```
<transportConnectors>
      [...]
      <transportConnector name="ssl" uri="ssl://0.0.0.0:61617?trace=false&amp;"
/>
</transportConnectors>
```

2. Add the certificate "broker-localhost.cert" to all Java keystores which should use this SSL connection with the following command:
   keytool -import -trustcacerts -keystore -storepass -alias activemq -import -file
3. Restart the ActiveMQ service
4. Restart the application which uses the updated keystore.

10.6 Clustering (optional)

The standard AMQ supports also the clustering topic, for more information please visit the the official Apache web page http://activemq.apache.org/clustering.html.

You can configure the **fail over** protocol for the JMS connector URL which is used in the Media Manager workflow(JMS client as producer) and Product 360 server(JMS client as consumer), so that a JMS client will connect to one of JMS brokers, then if the JMS broker goes down, it will auto-reconnect to another broker. And you can also create a Network of brokers to store and forward messages between brokers, so that messages could be always consumed even if they arrive at a broker without consumer. Such network can be defined directly in the broker's XML configuration (conf/activemq.xml by default). Take a look at the following snippet for example:

Configuring a network of broker

```
<beans
  xmlns="http://www.springframework.org/schema/beans"
  xmlns:amq="http://activemq.apache.org/schema/core"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans http://
www.springframework.org/schema/beans/spring-beans-2.0.xsd
  http://activemq.apache.org/schema/core http://activemq.apache.org/schema/core/
activemq-core.xsd">

    ...
    <broker xmlns="http://activemq.apache.org/schema/core" brokerName="amq1"
dataDirectory="${activemq.base}/data" destroyApplicationContextOnStop="true">
        ...
        <networkConnectors>
            <networkConnector name="amq1-nc"
            uri="static:(failover:(tcp://0.0.0.0:61617))"
            dynamicOnly="true"
            networkTTL="2"
            duplex="false">
                <!-- excluded audittrail destinations -->
                <excludedDestinations>
                    <queue physicalName="Consumer.ATCS.VirtualTopic.ATCS.ALL"/>
                    <topic physicalName="VirtualTopic.ATCS.ALL"/>
                </excludedDestinations>
            </networkConnector>
        </networkConnectors>

        <persistenceAdapter>
            <kahaDB directory="${activemq.base}/data/kahadb"/>
        </persistenceAdapter>

        ...

        <transportConnectors>
            <transportConnector name="openwire" uri="tcp://0.0.0.0:61616"/>
        </transportConnectors>

    </broker>
    <import resource="jetty.xml"/>
</beans>
```

ActiveMQ client uses failover transport for failover protocol . The Failover transport layers reconnect logic on top of any of the other transports. The configuration syntax allows you to specify any number of composite URIs. The Failover transport randomly chooses one of the composite URIs and attempts to establish a connection to it. If it does not succeed, or if it subsequently fails, a new connection is established choosing one of the other URIs randomly from the list. It retries connecting failover server unlimited number of times if used don't specify maxReconnectPatameters as below. Once max number parameter is passed then it

tries maximum number of reconnect attempts before an error is sent back to the client. The below sample queue url shows how to pass maxReconnectAttempts parameter.

queue.default.url = failover://(tcp://host:port)?maxReconnectAttempts=1

More about failover configuration parameters are mentioned in below doc.

https://activemq.apache.org/failover-transport-reference.html

ActiveMQ client library logs retry logic in a debug mode. If you want to enable these debug logger statements then you need to add below logger in log4j2.xml of PIM application.

<Logger name="org.apache.activemq" level="DEBUG" />

11 Media Manager Installation

Product 360 8.0 supports 2 different Digital Asset Management (DAM) Providers.

Theses DAM Providers are the classic provider and the Product 360 - Media Manager provider. The naming convention for these providers are:

- Product 360 - Media Manger for the Informatica Product 360 - Media Manager provider
- HLR for the classic provider

This document provides information on the installation of the Media Manager module and how to integrate it as Digital Asset Provider for Product 360.

11.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Setup Product 360 - Media Manager Database (see page 55)

11.2 Pre-Installation Checklist

11.2.1 OS User Permissions

11.2.1.1 Windows

- The users which install the Product 360 - Media Manager Modules need to be in the local Administrators group.

11.2.2 OS Volume Shares and Permissions

- hotfolder
- xmlspace

11.2.3 Default Product 360 - Media Manager Ports

Port	Protocol	Product 360 Module
11100	tcp	Funcd
11101	tcp	Pipe Funcd
11102	tcp	Internet Funcd
81	tcp	Product 360 Core and Product 360 - Media Manager Web - XOB Connection
8089	http	Session Manager, Web Status Page
8080	http	Product 360 - Media Manager Web, Product 360 - Media Manager REST
82	tcp	Product 360 - Media Manager Web XOB Connection (Administration) (optional for Product 360 8 only for upgrade)
83	tcp	Product 360 - Media Manager Web XOB Connection (Data) (optional for Product 360 8 only for upgrade)
84	tcp	Product 360 - Media Manager Web XOB Connection (Data) (optional for Product 360 8 only for upgrade)
8161	tcp	MessageQueue
61616	tcp	MessageQueue

Port	Protocol	Product 360 Module
8009	tcp	Product 360 - Media Manager Web, ajp13/mod_jk connector
59170 - 60678	tcp	Product 360 - Media Manager desktop modules (Workflowmanager) (see port range calculation below)
445 ,139	smb, tcp	Windows file share ports for the Product 360 Core and Product 360 - Media Manager file communication

11.2.3.1 Port range

Formula to calculate the port number of a module: **Portnumber = modulo(StationId,100) * 15 + 59169 + ModuleId**

==> New possible port range: 59170 - 60678

Module	Module Id	Port for Station 100	Port for Station 199
Process Watcher	1	59170	60655
Pipeline	2	59171	60656
Xob Adminconsole	3	59172	60657
Mediapublisher	4	59173	60658
Workflowmanager	5	59174	60659
XML Connector	6	59175	60670

Module	Module Id	Port for Station 100	Port for Station 199
Hotfolder	7	59176	60671
Archive	8	59177	60672
Interface	9	59178	60673
Medias	11	59180	60675
Production	12	59181	60676
Administration	14	59183	60678

11.3 Media Manager Installation

11.3.1 Installation checklist

11.3.1.1 New installation

This checklist names the minimum steps which are needed to install Product 360 - Media Manager:

- First install the Product 360 - Media Manager file server, refer to Installing Product 360 - Media Manager File Server (see page 111)
- The next step is to install the database, refer to Setup Product 360 - Media Manager Database (see page 55)
- The next step is to install the client modules, refer to Installing the client modules (see page 120) (important: restart the computer after installation)
- Install the Funcd, refer to Installing Funcd (see page 111)
- Installing the web front end (see page 123)
- Set up Product 360 - Media Manager, refer to Product 360 - Media Manager Configuration
- Optional (obsolete since Product 360 version 8): Setting up the Internet module (Internet Administration Console)
- Optional (obsolete since Product 360version 8): Setting up the Session Manager

11.3.1.2 Update

This checklist names the steps which are needed to update Product 360 - Media Manager:

- Updating Product 360 - Media Manager File Server
- Updating Product 360 - Media Manager database
- Updating the client modules
- Updating Funcd
- Updating web front end
- Updating rendering engines

11.3.2 Installing File Server

Before you can start using Product 360 - Media Manager, certain requirements must be met on the file server.

> The installation documentation is intended for Informatica system partners. In-proper handling can cause damage to the data and result in data losses.

Carry out the steps described below to set up the Product 360 - Media Manager volumes on your file server. To install the Product 360 - Media Manager database, you require the file **PIM_<*Version*>_MediaManager.zip** from your Product 360 distribution

1. Uncompress **PIM_<*Version*>_MediaManager.zip** from your Product 360 distribution to your local computer
2. Copy the **Volume0** directory to a server volume to which all client computers used have read and write access. The **Volume0** directory contains the example files for the sample company and the directory structure required for Product 360 - Media Manager.
3. In addition to **Volume0**, a BufferVolume must also be created, which is used to temporarily store pipeline conversions and as a spool directory for the funcd and backd programs. The recommended name for this buffer volume is **BufferVolume**. This folder has to be in the same directory as the **Volume0** folder. A template buffer volume matching the standard setup database resides in the main directory of your uncompressed zip file.

The procedure is different depending on whether you are using Windows or Macintosh OS X.

- Apple Macintosh OS X: Switch to the **Setup:HMM** directory and copy the **help%0** and update directories to **Volume0** on your file server, to the **opasdata** directory.
- Microsoft Windows: Run **SetupIMM.exe** in the setup directory on your Product 360 - Media Manager DVD and follow the instructions. Finally, rename the created folder from **updateYY_MM_DD** to **update**.

11.3.3 Installing Funcd

- General information (see page 112)
- File server Funcd (see page 112)
  - Windows (see page 113)
  - Linux (see page 113)
    - Prerequisites (see page 113)
    - Available Funcd archive (see page 113)
    - Step by step manual (see page 113)
    - Hints (see page 119)
      - Setting up ImageMagick under Red Hat Enterprise Linux 7 (see page 119)
      - Funcd port and the firewall (see page 120)
- Second Pipeline Funcd (optional) (see page 120)

11.3.3.1 General information

Before installing a new Funcd version you have to uninstall existing Funcd installations (see Update Product 360 - Media Manager). The Product 360 - Media Manager Funcd is a service, or a daemon, which executes the tasks requested by client modules. The commands used by the Funcd include the following, some of which are platform-specific:

- **layout** (Sun Solaris with Helios OPI support)
- **convert** (ImageMagic for all supported platforms)
- **exiftool** (Windows)
- Platform-specific copy commands (with dt-tools in the case of Helios support)

The client modules can communicate with the the Funcd via IP. Otherwise, the Funcd monitors a platform-specific input directory. The archive **PIM_<*Version*>_ThirdPartySoftware.zip** contains Funcd versions for the following platforms:

- Linux (funcd.linux)
- Windows 2008 R2 Server /Windows 2012 Server (funcd.nt)

Further information on setting up your Heiler Media Manager Funcd can be found in Activating Product 360 - Media Manager, defining volumes & setting up Funcd. Depending on the set debug level, the Funcd maintains a log with different levels of detail:

- 0 is the lowest debug level: No log is maintained.
- 20 is the highest debug level: An extremely detailed log is maintained.

The log file can be found in one of the following directories:

- **[...]/opastool/funcd**
- **[...]/opastool/funcdpip1**
- **[...]/opastool/funcdpip2**

Unless you make a different setting, the Funcd cancels any process with a timeout after 600 seconds with no response.

11.3.3.2 File server Funcd

Macintosh OSX and Linux

The Macintosh OSX or Linux packages are not part of the release package. You can get more information about these packages on request.

3rd party tools

Due to license restrictions GhostScript, ICC profiles, FFmpeg and MEncoder are not shipped with Informatica Media Manager.

Windows

> The folder **...\Volume0\opastool\funcd** is monitored by this Funcd. (It is recommended to use UNC paths.)

The procedure for installing the Informatica Media Manager Funcd for file servers on Windows Server is as follows:

1. Run the corresponding setup file in the directory **funcd.nt** on the third-party software CD: **Setup_FS_Funcd.exe**.
2. Click on **Next**.
3. Enter the path to the directory where the Funcd will be installed.
4. Click on **Next**.
5. The list of components that will be installed is displayed.
6. Click on **Next**.
7. Select the folder to be monitored, see note above.
8. Click on **Next**.
9. Configure the settings for TCP port, timeout, debug level and count of parallel processes. (It is not recommended to change the default values.) Please note the port, you will need it for the setting in the **Administration** module, see Activating Product 360 - Media Manager, defining volumes & setting up Funcd.
10. Click on **Next**.
11. Select the Start menu folder.
12. Click on **Next**.
13. Check that the installation routine has correctly identified the environment.
14. If all the information is correct, click on **Install**.
15. Exit the program.

The installation is complete.

Linux

Prerequisites

1. `Volume0` and `BufferVolume` from the main DVD must be residing in a share on the Linux server
2. `root` access
3. ImageMagick must be installed
4. ExifTool must be installed
5. Correct archive for your kernel version

Available Funcd archive

3RD_PARTY_CD/funcd.linux/RHEL_7.0/lnx_funcd_64_RH7.tgz

Step by step manual

1. Create a home directory for the Funcd

Create Funcd home

```
$ mkdir /opt/IMMfuncd
```

2. Unpack the Funcd archive in /opt/IMMfuncd

Unpack the Funcd archive

```
$ cd /opt/IMMfuncd
$ cp lnx_funcd_64_RH7.tgz .
$ tar -xzf lnx_funcd_64_RH7.tgz
```

3. Set access privileges for the complete funcd content

Set privileges

```
$ chmod -R 755 /opt/IMMfuncd
```

4. Move tools to Volume 0

Create {{tools}} folder

```
$ mkdir [...]/Volume0/opastool/funcd
$ mv tools [...]/Volume0/opastool/funcd
$ chmod 755 [...]/Volume0/opastool/funcd/tools/*.sh
$ chmod 755 [...]/Volume0/opastool/funcd/tools/convert
$ chmod 755 [...]/Volume0/opastool/funcd/tools/java/bin/*
```

5. Create links to ImageMagick in the `tools` folder

ImageMagick links

```
$ ln -s [path to ImageMagick]/convert [...]/Volume0/opastool/funcd/tools/convert2
$ ln -s [path to ImageMagick]/identify [...]/Volume0/opastool/funcd/tools/identify
$ ln -s [path to ImageMagick]/composite [...]/Volume0/opastool/funcd/tools/composite
$ ln -s [path to ImageMagick]/mogrify [...]/Volume0/opastool/funcd/tools/mogrify
```

ImageMagick location

Under Red Hat Enterprise Linux 7 the default location of ImageMagick is `/usr/bin`.

6. Create links to `tar` and `gzip` in the `tools` folder

{{tar}} and {{gzip}} links

```
$ ln -s [path to tar]/tar [...]/Volume0/opastool/funcd/tools/gtar
$ ln -s [path to gzip]/gzip [...]/Volume0/opastool/funcd/tools/gzip
```

tar and gzip locations

Under Red Hat Enterprise Linux 7 the default location of `tar` and `gzip` is `/bin`.

7. Create a link to Exiftool in the `tools` folder

Exiftool link

```
$ ln -s [path to exiftool]/exiftool [...]/Volume/oapstool/funcd/
tools/exiftool
```

Exiftool location

Under Red Hat Enterprise Linux 7 the ExifTool setup places ExifTool in `/usr/local/bin` by default.

8. Create the Funcd `init` script

Create {{init}} script

```
$ touch [path to init scripts]/IMMfuncd
```

init scripts location

Under Red Hat Enterprise Linux 7 the `init` scripts reside in `/etc/init.d`

9. Open the `init` script in an editor, e.g. `nano`

Open {{init}} script

```
$ nano [path to init scripts]/IMMfuncd
```

10. Copy & paste the following script in the editor and adapt the `PORT`, `CLIENTS`, `DEBUGLEVEL` and the `WORKDIR` to match your paths

Funcd {{init}} script

```
#!/bin/bash
WORKDIR=[...]/Volume0/opastool/funcd
BASEDIR=/opt/IMMfuncd
PORT=11000
CLIENTS=10
DEBUGLEVEL=20

PROG=funcd
OPTS="-d $WORKDIR -V $DEBUGLEVEL -p $PORT -C $CLIENTS"
FUNCD_HOME=$BASEDIR
export FUNCD_HOME

# Checking directories and executable
if [ ! -d ${BASEDIR} ]; then
  echo "ERROR: Base directory '${BASEDIR}' doesn't exist"
  exit 1
fi

if [ ! -x ${BASEDIR}/${PROG} ]; then
  echo "ERROR: Executable '${BASEDIR}/${PROG}' not found"
  exit 1
fi

if [ ! -d ${WORKDIR} ]; then
  echo "ERROR: Working directory '${WORKDIR}' doesn't exist"
  exit 1
fi

# Checking required tools
if [ ! -x ${WORKDIR}/tools/convert ]; then
  echo "ERROR: Executable '${WORKDIR}/tools/convert' not found"
  exit 1
fi

if [ ! -x ${WORKDIR}/tools/identify ]; then
  echo "ERROR: Executable '${WORKDIR}/tools/identify' not found"
  exit 1
fi

if [ ! -x ${WORKDIR}/tools/composite ]; then
  echo "ERROR: Executable '${WORKDIR}/tools/composite' not found"
  exit 1
fi

if [ ! -x ${WORKDIR}/tools/mogrify ]; then
```

```
46    echo "ERROR: Executable '${WORKDIR}/tools/mogrify' not found"
47    exit 1
48  fi
49
50  if [ ! -x ${WORKDIR}/tools/gtar ]; then
51    echo "ERROR: Executable '${WORKDIR}/tools/gtar' not found"
52    exit 1
53  fi
54
55  if [ ! -x ${WORKDIR}/tools/gzip ]; then
56    echo "ERROR: Executable '${WORKDIR}/tools/grip' not found"
57    exit 1
58  fi
59
60  if [ ! -x ${WORKDIR}/tools/exiftool ]; then
61    echo "ERROR: Executable '${WORKDIR}/tools/exiftool' not found"
62    exit 1
63  fi
64
65  # Start and stop functions
66  start() {
67    echo "Starting '$BASEDIR/$PROG $OPTS' ..."
68    cd $BASEDIR && ./$PROG $OPTS
69    RETVAL=$?
70
71    if [ $RETVAL -eq 0 ]; then
72      echo "  started"
73    else
74      echo "  Failure"
75    fi
76
77    echo
78    return $RETVAL
79  }
80
81  stop() {
82    echo "Stopping '$PROG' ..."
83    killall "$PROG"
84    RETVAL=$?
85    if [ $RETVAL -eq 0 ]; then
86      echo "  stopped"
87    else
88      echo "  Failure"
89    fi
90
91    echo
92    return $RETVAL
93  }
94
95  restart() {
96    stop
97    start
98  }
```

```

case "$1" in
  start)
    start
    ;;
  stop)
    stop
    ;;
  restart)
    restart
    ;;
  *)
    echo $"Usage: $0 {start|stop|restart}"
    RETVAL=1
esac

exit $RETVAL
```

11. Save the `init` script
12. Set access privileges for the `init` script

{{init}} access privileges

```
$ chmod 755 [path to init scripts]/IMMfuncd
```

13. Test the script and check the output
    a. Start the Funcd

Start the Funcd

```
$ [path to init scripts]/IMMfuncd start
Starting '[BASEDIR]/funcd -d [WORKDIR] -V [DEBUGLEVEL] -p [PORT] -C [CLIENTS]' ...

Parallel Funcd Linux Version [version number]
(C) 2002-2014 for Heiler Software AG by STORE! Media Enginieering
  started
```

    b. Check if the Funcd process is there

Check process

```
$ ps -e | grep funcd
15842 pts/2    00:00:00 funcd
```

> **Differing values**
>
> The values shown here are just an example. Most likely they will be different on your system.

c. Stop the Funcd

Stop the Funcd

```
$ [path to init scripts]/IMMfuncd stop
Stopping 'funcd' ...
  stopped
```

14. Link the `init` script to the desired run levels

Run level links

```
 $ ln -s [path to init scripts]/IMMfuncd [path to run level scripts]/rc[run level number].d/S90IMMfuncd
```

> **Run level location**
>
> Under Red Hat Enterprise Linux 7 the run level script links {{/etc/rc[run level number].d

15. If you do not want to reboot your system, start the Funcd now

Start the Funcd

```
$ [path to init scripts]/IMMfuncd start
Starting '[BASEDIR]/funcd -d [WORKDIR] -V [DEBUGLEVEL] -p [PORT] -C [CLIENTS]' ...

Parallel Funcd Linux Version [version number]
(C) 2002-2015 for Heiler Software AG by STORE! Media Engineering
  started
```

Hints

Setting up ImageMagick under Red Hat Enterprise Linux 7

Install ImageMagick using the built-in package manager `yum` is the easiest way to set up both of them.

Setting up ImageMagick under RHEL 7

```
$ yum install ImageMagick
```

Funcd port and the firewall

Remember to add a rule to your firewall that allows communication on the used Funcd port.

11.3.3.3 Second Pipeline Funcd (optional)

> The folder **...\Volume0\opastool\funcdpip1** is monitored by this Funcd. (It is recommended to use UNC paths.)

The procedure for installing the Heiler Media Manager second pipeline Funcd on Windows 2008 R2 Server/ 2012, XP or 7 is as follows:

1. Run the corresponding setup file in the directory **funcd.nt** on the third-party software CD: **Setup_PIP_Funcd.exe**.
2. Click on **Next**.
3. Enter the path to the directory where the Funcd will be installed.
4. Click on **Next**.
5. The list of components that will be installed is displayed.
6. Click on **Next**.
7. Select the folder to be monitored, see note above.
8. Click on **Next**.
9. Configure the settings for TCP port, timeout, debug level and count of parallel processes. (It is not recommended to change the default values.) Please note the port, you will need it for the setting in the **Administration** module, see Activating Product 360 - Media Manager, defining volumes & setting up Funcd.
10. Click on **Next**.
11. Select the Start menu folder.
12. Click on **Next**.
13. Check that the installation routine has correctly identified the environment.
14. If all the information is correct, click on **Install**.
15. Exit the program.

The installation is complete.

11.3.4 Installing the client modules

- Installing the client modules (see page 121)
  - Under Windows (see page 121)
  - Under Macintosh (see page 121)
- Installing and setting up the ODBC connection under Macintosh (see page 122)
  - Installation (see page 122)
  - Setup (see page 122)

11.3.4.1 Installing the client modules

To install new modules, mount Product 360 - Media Manager **Volume0** from the file server on your workstation and then follow the instructions below for your operating system.

> If you are installing new client modules or updating the version, you must re-activate Product 360 - Media Manager. For more details, refer to Activating Product 360 - Media Manager, defining volumes & setting up Funcd.

Under Windows

1. On **Volume0** on your file server, switch to the directory **opasdata/update/win/oclnt** (or MAIN_DVD\setup\HMM\update\win\oclnt)**.**
2. Run **OPAS_cln.exe.**
3. Follow the subsequent instructions.
4. Enter host string for your database:
   - Oracle: **//databaseserver:port/instance** (i.e. **//192.168.100.65:1521/hmm**)
   - MSSQL Server: For MSSQL the host string has to start with **MSSQL** and it has to be defined as an ODBC connection in the register User DSN. (i.e. **MSSQL_HMM**)
5. Type in your workstation number (i.e. the last 3 digits of your IP address)
6. Start the Administration module using **Program Files > Informatica Media Manager > Administration**.
7. Confirm all messages e.g. not mounted volumes.
8. Perform the activation; refer to Activating Product 360 - Media Manager, defining volumes & setting up Funcd.
9. You can log in using the user name **admin** and the password **sys**.

   > Change the administrator password as soon as possible.

10. Now make the local settings. For more details, refer to Product 360 - Media Manager Configuration.

Under Macintosh

1. On **Volume0** on your file server, switch to the directory **opasdata/update/osx**.
2. Mount the image **IMM.install.dmg**.
3. Run the Product 360 **- Media Manager** package installer.
4. Follow the subsequent instructions.
5. Start the Administration module using **Applications > Informatica Media Manager > Administration**.
6. Enter host string for your database:
   a. Oracle: **//databaseserver:port/instance** (i.e. **//192.168.100.65:1521/hmm**)
   b. MSSQL Server: For MSSQL the host string has to start with **MSSQL** and it has to be defined as an ODBC connection in the register Systen DSN. (i.e. **MSSQL_HMM**)
7. Type in your workstation number (i.e. the last 3 digits of your IP address)
8. Perform the activation.
9. You can log in using the user name **admin** and the password **sys**.

   > Change the administrator password as soon as possible.

10. Now make the local settings. For more details, refer to Product 360 - Media Manager Configuration .

11.3.4.2 Installing and setting up the ODBC connection under Macintosh

Product 360 - Media Manager supports access from OSX to a MSSQL database via the **ODBC Drivers Single-Tier (Lite Edition) (Release 6.1)** by OpenLink.

> The ODBC driver licenses are not included in the Product 360 - Media Manager license.

Installation

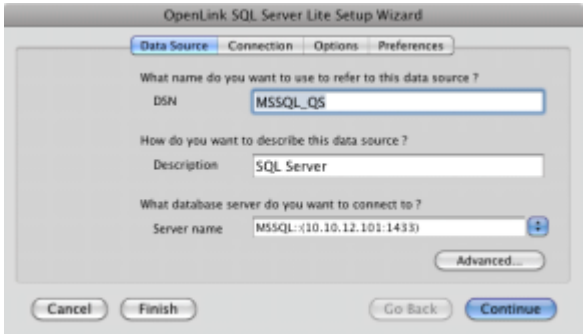
1. On **Volume0** on your file server, switch to the directory **opasdata/update/osx**.
2. Mount the image **mv16mzzz.dmg**.
3. Install the package **OpenLink-SQLServer-Lite.mpkg** following the instructions on the screen.
4. If the **SQLServerLiteInstaller** was started by the package installer the license file can be chosen.
5. Otherwise the license file **Licensfile** has to be copied to the directory **/Library/Application Support/openlink/bin**.

Setup

1. Start the program **OpenLink ODBC Administrator** located in the directory **Utilities** within the **Applications** directory.
2. Switch to the tab System **DSN** and click **Add**.

   > • This action requires administrative privileges.

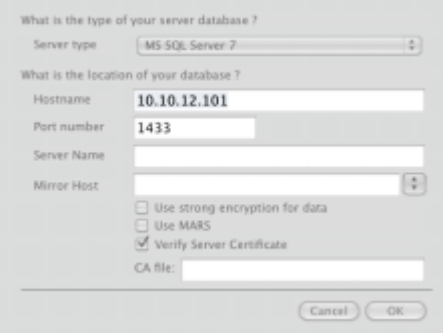
3. Select **OpenLink SQL Server Lite Driver (Unicode) V.6.X**.
4. Enter a DSN name.



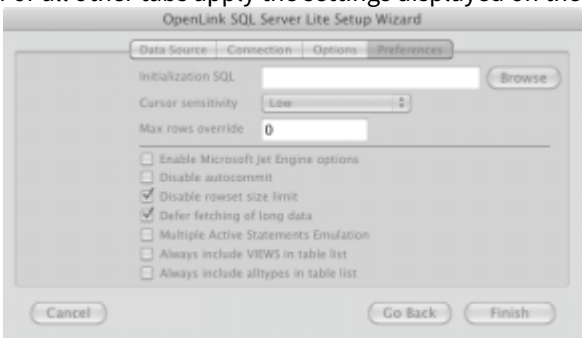
   > • The DSN name must begin with **MSSQL_**.

5. Click **Advanced**.
6. Select **MS SQL Server 7** as **Server type**.

7. Enter the hostname and port and click **OK**.



8. Apply the following settings to the tabs:
   - Tab **Connection**: Leave all settings and click **Continue**.
   - For all other tabs apply the settings displayed on the following screenshot.



9. Click **Finish**.

11.3.5 Installing the web front end

11.3.5.1 Windows

The procedure for setting up the Product 360 - Media Manager web front end on Windows is as follows:

1. On your Product 360 - Media Manager installation directory, switch to the directory **\setup\webapp package\full**.
2. Unpack the file **OpasGWebServer.zip** to **C:**.
3. In the file **C:\OpasGWebServer\Tomcat\webapps\opas\Base.cfg**, enter the database connection parameters.
   <DATABASE_URL>jdbc:sqlserver://localhost:1433;databaseName=opasdb</DATABASE_URL (see page 123) **>**
   <DATABASE_DIALECT>org.hibernate.dialect.SQLServer2012Dialect</DATABASE_DIALECT>
   <DATABASE_USER>Username</DATABASE_USER>
   <DATABASE_PASSWORD>Password</DATABASE_PASSWORD>
4. Launch Tomcat using the script **C:\OpasGWebServer\startup.bat**.

You can also run Tomcat as a Windows service; refer to Run Product 360 - Media Manager server modules as a Windows service .

MSSQL with encrypted connection

It is possible to use an encrypted connection to the Media Manager database (MSSQL only). Append ';encrypt=true' to your url.

The url would look like

```
jdbc:sqlserver://localhost:1433;databaseName=opasdb;encrypt=true
```

To use this feature the MSSQL DBMS has to have a setup encryption mechanism.

MSSQL with integrated security

It is possible to use the integrated security feature between Windows and MSSQL. To use integrated security just enter no **DATABASE_USER** and **DATABASE_PASSWORD** values. In that case the Windows user which runs the Tomcat service is used to logon to the database. Please be sure your database allows access to this Windows user.

If only the Media Manager web front end is running in the Tomcat you use the default installation and leave the database credentials empty.

MSSQL Integrated security running Media Manager web front end and Media Manager Rest services in one Tomcat

Beside the Media Manager web front end sometime the Media Manager Rest services (used for Supplier Portal) running in the same Tomcat. In that case some additional steps are necessary to enable the integrated security for both web applications.

Preconditions

- Installed and setup OpasGWebServer: Your web front end is running and is usable with database credentials
- Installed and setup Media Manager Rest services inside the OpasGWebServer: The Rest services are usable with database credentials.

Steps to enable integrated security for both web applications

1. Create a new folder '`sharedLib`' at `OpasGWebServer\Tomcat`
2. Move '`mssql-jdbc-7.2.2.jre8.jar`' from `OpasGWebServer\Tomcat\webapps\opas\WEB-INF\lib` to `OpasGWebServer\Tomcat\sharedLib`
3. Open `OpasGWebServer\Tomcat\conf\catalina.properties` in a text editor and change line `shared.loader=`

to
`shared.loader=${catalina.base}/sharedLib/*.jar`

4. Delete '`mssql-jdbc-7.2.2.jre8.jar`' from
`OpasGWebServer\Tomcat\webapps\rest\WEB-INF\lib`
5. Now you can replace the database credentials in the configuration files with empty values
`OpasGWebServer\Tomcat\webapps\opas\Base.cfg`
`OpasGWebServer\Tomcat\webapps\rest\WEB-INF\classes\META-INF\spring\hmm-database.properties`

> **Why is that necessary?**
>
> Integrated security is realized by a dll. A dll can be loaded only by one classloader. Our 2 web applications running in 2 different classloaders. This cause problems if 2 applications try to load the same dll.
>
> By using the shared library mechanism of Tomcat it is possible to use the same dll in multiple web applications.

11.3.5.2 Linux

This page describes how to install the webapplication of Media Manager on Linux (Redhat 7).

Installation

1. On your Product 360 - Media Manager installation directory, switch to the directory **\setup\webapp package\full**.
2. Copy package OpasGWebServerLinux.zip to /opt
3. Unzip this package to /opt

```
$ cd /opt
$ unzip OpasGWebServerLinux.zip
```

4. Set attributes to make scripts executable

```
$ chmod 777 /opt/OpasGWebServer/*.sh
$ chmod 777 /opt/OpasGWebServer/Tomcat/bin/*
$ chmod 777 /opt/OpasGWebServer/java/bin/*
```

5. Change owner of installed package to service user

```
1  $ chown -R serviceuser /opt/OpasGWebServer
```

6. Configure database connection in **`/opt/OpasGWebServer/Tomcat/webapps/opas/base.cfg`** .
   <DATABASE_URL>**jdbc:oracle:thin:@dbervername:1521:oracle_instance**</DATABASE_URL>
   <DATABASE_DIALECT>org.hibernate.dialect.Oracle10gDialect</DATABASE_DIALECT>
   <DATABASE_USER>OPASUSER</DATABASE_USER>
   <DATABASE_PASSWORD>**Password**</DATABASE_PASSWORD>
7. start server

```
1  $ su - serviceuser
2  $ /opt/OpasGWebServer/Tomcat/bin/tomcat start
```

Install / Remove service

The web application has a preconfigured service wrapper inside. To install this application as a service do the following steps.

```
1  $ su - serviceuser
2  $ /opt/OpasGWebServer/Tomcat/bin/tomcat install
3  or to remove
4  $ /opt/OpasGWebServer/Tomcat/bin/tomcat remove
```

console output

```
1   []# /opt/OpasGWebServer/Tomcat/bin/tomcat install
2   Detected RHEL or Fedora:
3   Installing the Informatica Media Manager Web Application daemon..
4
5
6   []# /opt/OpasGWebServer/Tomcat/bin/tomcat remove
7   Detected RHEL or Fedora:
8   Stopping Informatica Media Manager Web Application...
9   Informatica Media Manager Web Application was not running.
10  Removing Informatica Media Manager Web Application daemon...
```

Configuration: mount volumes

You have to mount and link every used share of every file server. If you defined more volumes in one share, then you need only one mount for all these volumes.

Have a look in your Media Manager Administration 'system volumes': how you configured the unc path.

Example for the UNC Path in Administration: /FileserverOrIP/OpasVolumes/Buffer

```
$ mkdir /mnt/FileserverOrIP
$ mkdir /mnt/FileserverOrIP/OpasVolumes
$ mount -t cifs -o username=remoteserviceuser //
FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/OpasVolumes
$ ln -s /mnt/FileserverOrIP /FileserverOrIP
```

If you want to mount the volumes permanently, you can add them to /etc/fstab

1. Open /etc/fstab with your favorite editor
2. Add the following line to the end of the file

```
//FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/
OpasVolumes cifs
user=remoteserviceuser,uid=localserviceuser,gid=localservi
cegroup 0 0
```

If the password is required to mount the Volume, this solution is not working. You can change the line to:

```
//FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/
OpasVolumes cifs
user=remoteserviceuser,password=pass,uid=localserviceuser,
gid=localservicegroup 0 0
```

or to

```
//FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/
OpasVolumes cifs
user=remoteserviceuser,uid=localserviceuser,gid=localservi
cegroup,noauto 0 0
```

With the first solution the Volume will be mounted on every startup.
With the second solution the volume won't be mounted on startup. It can be mounted with:

```
$ mount /mnt/FileserverOrIP/OpasVolumes
```

Modify fstab without reboot.

To reload the contents of `fstab` without reboot use the following command.

```
mount -a
```

Configuration: base.cfg

Optional: Install ImageMagick

If you want to generate templates for the Media Manager web UI it is necessary to install ImageMagick.

1. Use yum to install ImageMagick

```
$ yum install ImageMagick
```

2. Edit colorme-Skript

```
$ cd /opt/OpasGWebServer/Tomcat/webapps/opas/custom/profiles/layout/template/
$ rm colorme.sh
$ cp colorme.sh_disabled colorme.sh
$ chmod 777 colorme.sh
```

3. Create symbolic links to ImageMagick-commands

```
$ cd /opt/OpasGWebServer/Tomcat/webapps/opas/custom/profiles/layout/template/imagemagick/
$ ln -s /usr/bin/composite composite
$ ln -s /usr/bin/convert convert
$ ln -s /usr/bin/montage montage
```

Optional: Configure XOB

If you want to use the projects engine it is necessary to mount the xob-workspace.

```
$ mkdir /mnt/FileserverOrIP
$ mkdir /mnt/FileserverOrIP/xobWorkdir
$ mount -t cifs -o username=serviceuser //FileserverOrIP/xobWorkdir/mnt/FileserverOrIP/xobWorkdir
$ mkdir /FileserverOrIP
$ ln -s /mnt/FileserverOrIP /FileserverOrIP
```

11.3.5.3 Encrypted passwords in configuration files

Product 360 Media Manager Web supports the encryption of secure information like passwords in the configuration files `Base.cfg` and `HPMConfig.xml`. The encryption will be executed only if your secure information in the configuration files is enclosed by the marker `[_to_encrypt_]`.
So, if you want to have e.g. the password "Password" encrypted in a configuration file just use the marker before and after the password like this: `[_to_encrypt_]Password[_to_encrypt_]`. Please note first encryption gets done with the first configuration file access. This means the `Base.cfg` gets encrypted by the first load of the login page. The `HPMConfig.xml` after the first login.

For example in `Base.cfg`:

properties file

```
<DATABASE_URL>jdbc:oracle:thin:@dbervername:1521:oracle_instance</DATABASE_URL>
<DATABASE_DIALECT>org.hibernate.dialect.Oracle10gDialect</DATABASE_DIALECT>
<DATABASE_USER>OPASUSER</DATABASE_USER>
<DATABASE_PASSWORD>[_to_encrypt_]Password[_to_encrypt_]</DATABASE_PASSWORD>
```

Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information

Product 360 Media Manager Web provides a default implementation for the encryption of secure information with an internal and securely stored Key using AES-256.
For sophisticated deployments we recommend to integrate with Encryption Key Management solutions like Amazon AWS or Azure KeyVault and use the API we offer to send and receive data for encryption to these key stores securely.

11.3.6 Setting up PIM - Media Manager

The steps to configure (setting up) are described in: Media Manager Configuration

11.4 Media Manager Integration

- Product 360 - Server (see page 130)
  - Integrating Product 360 - Media Manager (see page 130)
    - Switching default media asset provider to Product 360 - Media Manager (see page 130)
    - Configuring Product 360 - Media Manager (see page 130)
      - Connection data (see page 131)
      - Shares (see page 133)
      - Notification queue (see page 133)
      - Write access (see page 134)
      - Additional language packages (see page 135)
      - Miscellaneous (see page 136)
      - Auto Assignment (see page 137)

- Configuration example of Product 360 - Media Manager (see page 137)
- Using Product 360 - Media Manager with master assets and derivates (see page 140)
- Adding new media asset attribute(property field) to the repository (see page 141)
  - Add new media asset attribute(property field) for media asset file (see page 142)
  - Add new media asset attribute(property field) for media asset document (see page 142)
- Product 360 - Desktop Client (see page 143)

11.4.1 Product 360 - Server

11.4.1.1 Integrating Product 360 - Media Manager

The usage of Product 360 - Media Manager as media asset provider for Product 360 - Server presumes that Product 360 - Media Manager has been installed. Please refer to the Product 360 - Media Manager installation manual for such an installation.

Product 360 - Media Manager is integrated into the Product 360 - Server by means of a plug-in. This plug-in is default installed and must be configured afterwards. The following chapters will explain this in detail.

Switching default media asset provider to Product 360 - Media Manager

In order that Product 360 - Server uses Product 360 - Media Manager as media asset provider, you have to switch the default media asset provider to Product 360 - Media Manager. This is performed in the C:\Informatica\server\configuration\HPM\server.properties file by setting the "mime.defaultProvider" parameter in the "Media Asset Server (MAS) Settings" section to "HMM":

```
##############################################################################
### Media Asset Server (MAS) Settings
# Defines the default provider for media assets which defines the source where to
obtain the multimedia documents from(e.g. HLR, HMM).
# MediaAssets are administered by a provider. A implement of provider is already
included by standard HPM(Identifier=HLR).
# The identifier of provider is defined in its plugin.xml, see the Extension point
com.heiler.ppm.mediaasset.server.mediaAssetProvider.
# If no provider is explicit specified, then the here defined default provider will
be used.
mime.defaultProvider = HMM
```

Configuring Product 360 - Media Manager

After the integration of the Product 360 - Media Manager plug-in, you have to configure the plug-in to your needs. The configuration should be performed in the C:\Informatica\server\configuration\HPM\hmm.properties file.

The parameters concerning the Product 360 - Media Manager configuration can be found in the "connection settings for the application server" section.

The following sections describe the configuration parameters.

Special characters

If a value contains unicode characters store them using escape sequences, e.g. \u00C4 for the German umlaut Ä.

Connection data

In order that Product 360 server can connect to Product 360 Media Manager, you have to specify the corresponding settings for Product 360 - Media Manager and it's database.

The following table lists the connection parameters:

MSSQL - Integrated security

If your security guidelines do not allow passwords in configuration files you can use integrated authentication on Windows operating systems. (MSSQL only)

Property	Description
`hmm.login.supervisor.userName`	Login name of the supervisor user at Media Manager who has all rights and will be mapped to the Product 360 administrator.
`hmm.login.supervisor.password`	Password of the supervisor user at Media Manager who has all rights . If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
`hmm.login.customer`	Customer ID for the authentication at Product 360 - Media Manager.

Property	Description
`hmm.db.url`	Url of the Media Manager database which can be reached by Product 360. It is possible to use an encrypted connection to the Media Manager database (MSSQL only). Append ';ssl=request' to your url. The url would look like `jdbc:sqlserver://localhost:1433;databaseName=opasdb;ssl=request`
`hmm.db.user`	Login name at the Media Manager database which can be reached by Product 360. Might be empty if integrated authentication with MSSQL is used.
`hmm.db.password`	Password for the above mentioned user at the Media Manager database which can be reached by Product 360. Might be empty if integrated authentication with MSSQL is used.
`hmm.db.type`	Supported Product 360 - Media Manager database type. It must be one integer of the following values: **1**: ORACLE 11g R2 and above; **2**: MSSQL SERVER 2008 R2; **3**: MSSQL SERVER 2012 and above
`hmm.db.allowAutomaticMigration`	Specifies whether the Informatica Media Manager database gets updated automatically during the P360 starts up a connection with it. Default is true.
`hmm.connection.poolsize`	Size of connections pool per Product 360 user to Media Manager, default value is 10.

Property	Description
`hmm.connection.timeoutSEC`	Time out setting(in seconds) for each connection to Media Manager. The connection will be deleted after this period. Default value is 1800.

Shares

Product 360 - Server uses one share within the Product 360 - Media Manager system for accessing exported media assets. In order that Product 360 - Server can access this share, its path must be declared.

Property	Description
`hmm.share.export` Removed since Product 360_8.0.03	Path to the share containing the temporary exported zip file for images. This share must provide read-write access to application server.

Please note that the local directories of the shares might not (yet) exist. Usually the Product 360 - Server creates these directories on the first start, but for this configuration step you would need to do this manually to be able to create the share on them.

Notification queue

If Product 360 - Server should use the master asset functionaltity of Product 360 - Media Manager, Product 360 - Server must keep itself informed about asset changes in Product 360 - Media Manager by listening to corresponding notification queues.

In order that this mechanism works, the following parameters have to be configured:

Property	Description
`hmm.jms.connection.url`	Connection URL to Media Manager JMS server which replaces the old settings for notification queue. An error message for unreachable JMS server is only ensured with the transport options "initialReconnectDelay" and "maxReconnectAttempts". **Example** hmm.jms.connection.url = failover:(tcp://JMSServer:61616?wireFormat.maxInactivityDuration=0)?initialReconnectDelay=2000&maxReconnectAttempts=2
hmm.jms.connection.username	Optional property as the name for the authentication user during connection to the Media Manager JMS server. They are only necessary if the user should be authorized to connect to the Media Manager JMS server. This property is introduced only for the cloud solution, therefore it is currently not available since the media manager still connects to JMS server without authorization mechanism.
hmm.jms.connection.password	Optional property as the password for the authentication user during connection to the Media Manager JMS server. They are only necessary if the user should be authorized to connect to the Media Manager JMS server. This property is introduced only for the cloud solution, therefore it is currently not available since the media manager still connects to JMS server without authorization mechanism.

Write access

If Product 360 - Server should be supported with the wirte access of Product 360 - Media Manager, the following parameters have to be configured:

Property	Description
`hmm.supportsWrite`	Set this to false, If the write access of media manager Provider should not be supported. Please note, that there is not granular destinction. Either the Provider supports FULL write support (Upload, Removing files and categories...) or doesn't support write at all. **Default value** true
`hmm.defaultCategoryId`	The identifier of default category(usually names "Unassigned") which stores all images that are not assinged to other categories. The default category id can be fetched by calling the following sql statement from the Media Manager database: select IHIE_ID from F_IMGHIER where IHIE_NAME = 'Unassigned'

Additional language packages

If you have installed additional language packages (refer to appendix "i18n language packages" for more information), you will have to add respective mappings into the hmm.properties file. This is due to the fact that Product 360 -Server works with locales and Product 360 - Media Manager with language numbers.

The mapping entries must look like this:

```
# Mapping from Locales to Media Manager language numbers
hmm.locale.en_US=0
```

- A setting with false value can cause fatal error by fetching asset information form Media Manager!
- locale must be an enum entry defined in the enumeration "Enum.Language".

Tip: The language numbers are defined in the "Informatica Product 360 Media Manager Administration". You can retrieve a list of the language numbers from by selecting "System" -> "Manage languages" in the native application "Informatica Product 360 Media Manager Administration"

Miscellaneous

The following table lists all other parameters for the configuration of the Product 360 - Media Manager plug-in:

Property	Description	Default value
`hmm.maxCountOfIdsInOneThread`	Maximum count of ids which are sent as parameter to corresponding connector API call that can be run with multi-threading. This value can be adjusted in real time for a better performance. For more detailed information please visit the section "Media Asset Parallel Management" of chapter "Tuning advisory" in [OpertationManual].	1000
`hmm.numberOfThread.initValue`	This setting defines the initial vlaue for the number of threads which are used for calling media asset parallel operations. Default value is 1, therefore this initial value should be adjusted according to the corresponding hardware and media manager configuration(e.g. number of hmm port). After start of the Product 360 - Server, the value of numberOfThread can be also changed by JMX tooling in real time.	1
`hmm.maxNumberOfDisplayableObjects`	Maximum number of the from Product 360 - Media Manager loadable media objects pro search, no matter what default value in the Product 360 - Media Manager system parameters.	10000
`defaultquality`	The default image quality. This parameter is only needed when using the master asset functionality of Product 360 - Media Manager.	originalimage

Property	Description	Default value
`hmm.exportMediaAsset.defaultWithLoggedInUser` available since 8.0.01.04, 8.0.03.00	Specifies whether the logged in user will be used as default while exporting media asset information from the Media Manager. If it is set as true, then only the media assets will be exported, which can be accessed by the logged in user who runs the export job. Otherweise the media assets will be exported, which can be accessed by the defined system user(system user has the access level of the Media Manager user defined with the "hmm.login.supervisor.userName").	true
`hmm.exportMediaAsset.uncpath.separator` available since 8.0.03.01(Version 8.0 Update 3 Hotfix 01)	Specifies which separator should be used in the unc path returned from the corresponding methods of Media Manager provider for export. Default is the backslash("\\"), if you want to use the unc path directly under Unix system, please set it with the slash("/")	\\

Auto Assignment

All settings for Auto Assignment and Auto path resolution please visit the page: Configurations for Auto Assignment

Configuration example of Product 360 - Media Manager

Example for hmm.properties(without auto assignment configurations)

```
################################################################################
### connection settings for the application server
### --------------------
### Connection data
#
# supervisor user in media manager with all rights
# hmm.login.supervisor.userName=<ENTER SUPERVISOR USERNAME HERE>
```

```
# hmm.login.supervisor.password=<ENTER SUPERVISOR PASSWORD HERE>
hmm.login.supervisor.userName=toto
hmm.login.supervisor.password=toto
#
# Identical customer ID which is defined in Media manager for all media manager users
who will be mapped to corresponding Product 360 user.
# hmm.login.customer=<ENTER MEDIA MANAGER CUSTOMER NUMBER HERE, e. g. D120001>
hmm.login.customer=D080001
#
# hmm.db.url=<ENTER MEDIA PORTAL DATABASE CONNECTION URL HERE, e. g.
jdbc:<server_type>://<server>[:<port>][;databaseName=<database>]>
# hmm.db.user=<ENTER MEDIA PORTAL DATABASE USERNAME HERE>
# hmm.db.password=<ENTER MEDIA PORTAL DATABASE PASSWORD HERE>
# supported database type: 1 = ORACLE 11g R2 and above
#                          2 = MSSQL SERVER 2008 R2
#                          3 = MSSQL SERVER 2012 and above
# hmm.db.type=<ENTER MEDIA PORTAL DATABASE TYPE HERE, e. g. 2>
hmm.db.url=jdbc:sqlserver://10.10.11.198:1433;databaseName=opasdb
hmm.db.user=totoUser
hmm.db.password=totoPassword
hmm.db.type=2
#
# size of connections pool per HPM user to Media Portal
hmm.connection.poolsize=10
# time out setting(in seconds) for each connection, the connection will be deteled
after this period
hmm.connection.timeoutSEC=1800
#
### --------------------
### Notification queue
#
# Connection URL to Media Manager JMS server
# Default protocol prefix is 'failover:' to ensure a robust connection, and the
default transport Options are initialReconnectDelay=2000&maxReconnectAttempts=2,
# so that after 2 attempts at connecting an exception will be shown to user who
decides reconnection again or restart the Product 360 server after correcting this
 url.
# The further default connection option is '?wireFormat.maxInactivityDuration=0' to
increase robustness
# Example for JMS server '10.10.11.198' and port '61616':
# hmm.jms.connection.url=failover:(tcp://10.10.11.198:61616?
wireFormat.maxInactivityDuration=0)?initialReconnectDelay=2000&maxReconnectAttempts=2
hmm.jms.connection.url=failover:(tcp://10.10.11.198:61616?
wireFormat.maxInactivityDuration=0)?initialReconnectDelay=2000&maxReconnectAttempts=2
#
### --------------------
### Write access
#
# Set this to false, If the write access of HMM Provider should not be supported,
default value is true.
# Please note, that there is not granular destinction.
```

```
# Either the Provider supports FULL write support (Upload, Removing files and
categories...) or doesn't support write at all.
hmm.supportsWrite = true
#
# hmm.defaultCategoryId indicates the identifier of default category(usually names
"Without Category") which stores all images that are not assinged to other
categories.
hmm.defaultCategoryId =
0068000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000
#
### --------------------
### Additional language packages
#
# Mapping from Locales to HMM language numbers
# Caution: a setting with false value can cause fatal error by fetching asset
information form HMM!
# Tip: The language numbers are not fix, but are set by the "Product 360 - Media
Manager Administration".
# You can retrieve a list of the language numbers from by selecting System > Manage
languages in the native application "Product 360 - Media Manager Administration"
hmm.locale.en_US=0
#
### --------------------
### Miscellaneous
#
# maximum count of ids which are send as parameter to corresponding XOB Call that can
be run with multi-threading
hmm.maxCountOfIdsInOneThread = 1000
#
# Initial value for the number of threads which are used for all media asset parallel
operations.
# Default is 1, therefore this initial value should be adjusted according to the
corresponding hardware and media portal configuration(e.g. number of hmm port).
# After start of the hpm server, the value of numberOfThread can be also changed by
JMX tooling in real time.
hmm.numberOfThread.initValue =1
#
# This properties defines the maximum number of the from HMM server loadable media
objects pro search, no matter what default value in the HMM system parameters.
hmm.maxNumberOfDisplayableObjects = 10000
#
# The default quality(master asset) of the provider
defaultquality=originalimage
#
# Specifies whether the logged in user will be used as default while exporting media
asset information from the Media Manager.
# false - the media assets will be exported, which can be accessed by the defined
system user(system user has the access level of the Media Manager user defined with
the "hmm.login.supervisor.userName").
# true - default / only the media assets will be exported, which can be accessed by
the logged in user who runs the export job.
```

```
hmm.exportMediaAsset.defaultWithLoggedInUser=true
#
# Specifies which separator should be used in the unc path returned from the
corresponding methods of Media Manager provider for export.
# Default is the backslash("\\"), if you want to use the unc path directly under Unix
system, please set it with the slash("/")
hmm.exportMediaasset.uncpath.separator =\\
```

Using Product 360 - Media Manager with master assets and derivates

Product 360 supports the master asset business logic provided by Product 360 - Media Manager.

This implies that Product 360 - Server must be informed about new derivate shemas or changes in existing derivative shemas performed in the integrated Product 360 - Media Manager. Product 360 - Media Manager keeps Product 360 - Server informed about such changes by putting respective notifications into its notification queues.

Product 360 - Server can obtain these notifications by means of a listener listening to this notification queue. In order that this mechanism works, the notification queue parameters as well as the `defaultquality` parameter must be correctly set in the `hmm.properties` file.

> After Product 360 - Server has collected or successfully consumed a notification, the notification is removed from the notification queue.

There are several notifications which can currently be processed by the Product 360 - Server. It is necessary that you check that the following notification queue events are configured in the workflow manager of Product 360 - Media Manager:

- **Notifications from the queue "heiler.hmm.backend.event"**
  - **Changed derivative schema (name)** The listener listens to the notification queue on the topic "ModifyDerivativeSchema" for a "F_DERIVATE.DEV_ID" which has to be a number (the number of the changed derivative schema id). The listener triggers only a change of the derivative schema name in the "MediaAssetQualityEnumeration".
  - **New derivative schema** The listener listens to the notification queue on the topic "NewDerivativeSchema" for a "F_DERIVATE.DEV_ID" which has to be a number (the number of the new created derivative schema id). The listener triggers a creation of new media asset documents on a media asset if this media asset has a mapped master asset and the derivative of this asset is just calculated by the pipeline. Furthermore, the listener triggers an update of the "MediaAssetQualityEnumeration".
  - **Delete derivative** The listener listens to the notification queue on the topic "DeleteDerivative" for a "F_DERIVATE.DEV_ID" which has to be a number (the number of a derivative schema id) and for the "F_IMGKOMP.PKOM_PNR" (the master asset identifier). The listener triggers a deletion of all to Product 360 object assigned media asset document for the corresponding master asset identifier and quality(derivative schema id). Typically this notification is sent if the pipeline has deleted a derivative.
- **Notifications from the queue "heiler.hmm.backend.event.assignment"**
  - **Assign document** The server job "AssignDocumentJob" picks the next message up from the notification queue, if it has the topic "AssignDocument" with a property "F_IMGKOMP.PKOM_PNR" which has to be a string(the identifier of the media asset), a "F_IMGKOMP.PIMG_SOURCE_FILENAME" which has to be a string(the name of the media asset), and a "F_IMGKOMP.PIMG_CATALOG_ID" which

has to be a string(the identifier of the catalog), the the server job triggers an assignment of corresponding media asset document to a Product 360 catalog object.
    - **New derivative of a media asset** The server job "AssignDocumentJob" picks the next message up from the notification queue, if it has the topic "NewDerivative" with a property "F_DERIVATE.DEV_ID" which has to be a number (the number of a derivative schema id) and a "F_IMGKOMP.PKOM_PNR" which has to be a string(the master asset identifier). The server job triggers a creation of a new media asset document on the media assets which contain the master asset identifier in a media asset document which has the master asset quality (e.g. originalimage). Typically this notification is sent if the pipeline has rendered a derivative quality.
- **Notifications from the queue "heiler.hmm.backend.event.assetModified"**
    - **Asset modified** The server job "UpdateModifiedAssetJob" picks the next message up from the notification queue, if it has the topic "AssetModified" with a property "F_IMGKOMP.PKOM_PNR" which has to be a string(the identifier of the changed media asset), the server job triggers the update of the "modificationTimestamp" for the corresponding media asset documents, meida assets and assinged objects(item, product and structure group).

There are example workflows existing which can be imported into the Product 360 - Media Manager workflow manager.

> The corresponding example workflows contains also another useful workflows which should be adjusted and imported into the Product 360 - Media Manager workflow manager. Especially the workflow "Automatic group assignment" should be actived to automatically assign all unassigned images(images which are not assigned to any other category) to the default category. For more details information please visit the page Media Manager Workflows.

How to work with workflows and how to change and modify workflows inside the workflow manager is described in the Product 360 - Media Manager manual and is only supported by the Product 360 - Media Manager consulting and support teams.

> To enable the message queue on the Product 360 - Media Manager side you have to start the activemq script on the Product 360 - Media Manager server by executing the startup.bat.

Adding new media asset attribute(property field) to the repository

The Product 360 - Server has read/write access to the media asset attributes of Product 360 - Media Manager.

Since the configuration of the Product 360 - Server repository is adjusted to the current state of supported media asset attributes, it might be necessary to add some (user defined) attributes.

> Only the property field(meta data definition) of Product 360 - Media Manager can be added in Product 360 core in this way!

This chapter describes how you can do this. It is assumed that you have installed the repository editor from the setup archive

```
PIM_<Version>_Rev-<Revision>_repoEdit_<OS>.zip, e.g.
PIM_8.0.00.00_Rev-12345_repoEdit_win32.zip
```

To add new media asset attributes to the Product 360 - Server repository, perform the following steps:

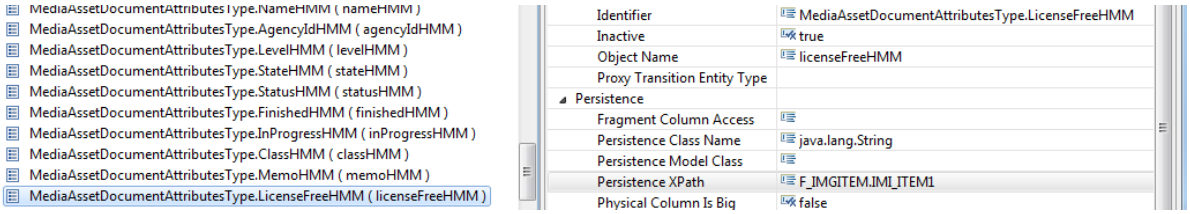
Add new media asset attribute(property field) for media asset file

Please visit the following page for detailed information: Bring Media Manager property field in media asset file views of PIM desktop.

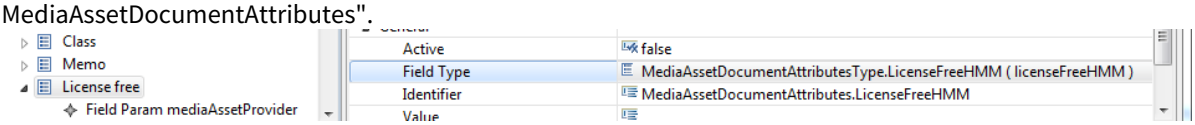
Add new media asset attribute(property field) for media asset document

1. Open the C:\Informatica\server\configuration\HPM\Repository.repository file in the repository editor.
2. In the "types" area, add an new field type under the entity type "MediaAssetDocumentAttributesType".

   Note: The value of "Persistence XPath" is the identifier of corresponding Product 360 - Media Manager field, e.g. "F_IMGITEM.IMI_ITEM1" is the identifier for the first meta data value of asset, and so on.

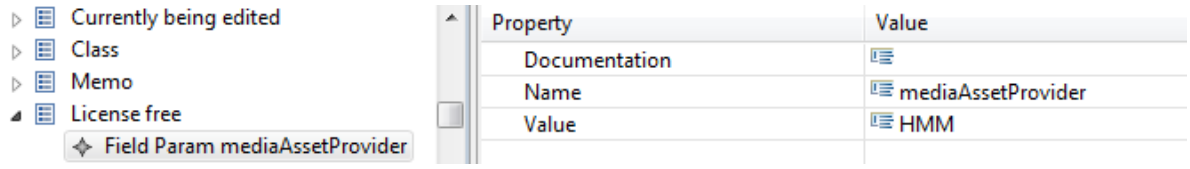
   

3. In the "custom" area, add an new field of the defined field type under the entity "MediaAssetDocumentAttributes".

   Currently only read access is supported for the fields under the entity "MediaAssetDocumentAttributes", therefore the corresponding "Editable" property has to be set with "false".

   Note: Add a field parameter under the field which has as key "mediaAssetProvider" and as value: "HMM" (this is necessary for the automatic detection of the necessary fields by the Product 360 - Server)

4. Add the respective field identifier with the language dependent name for each added field to the C:\Informatica\server\configuration\HPM\Repository.properties_[language key] (e.g. C:\Informatica\server\configuration\HPM\Repository.properties_en) files.

> Note: Since Product 360 version 7.0.03 the media asset attribute with type "multiple selection list" can be also shown in Product 360 - Desktop client, for that the "Upper Bound" of the corresponding field type in repository must be set as "-1".

11.4.2 Product 360 - Desktop Client

The respective plug-in on the client side which integrates the Media Manager web view in Product 360 Desktop, is not supported in standard Product 360 solution any more. If any reqular customer has always such request, please contact your administrator or our support.

12 Supplier Portal Installation

Please follow the predefined order of the following subsection to prepare the individual Informatica PIM modules for use with the Informatica PIM - Supplier Portal.

- Pre-Installation Checklist (see page 143)
- Supplier Portal Integration (see page 145)
- Media Manager and Supplier Portal Integration (see page 172)
- Web and Supplier Portal Integration (see page 178)
- Server Installation on Windows (see page 179)
- Server Installation on Linux (see page 187)
- Language Pack Installation (see page 195)
- Installation Troubleshooting (see page 195)

12.1 Pre-Installation Checklist

12.1.1 OS User Permissions

12.1.1.1 Windows

- The users which installs the Product 360 - Supplier Portal need to be in the local Administrators group.
- You need read/write permissions for the **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>** directory.
- The windows service user which runs the Product 360 - Supplier Portal Tomcat, needs also read/write permissions for the **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>** directory.

12.1.1.2 Linux

- The users which installs the Product 360 - Supplier Portal requires root privileges.
- The service user need read/write permissions for the **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>** directory.

> We recommand to create an service user to run the Product 360 - Supplier Portal under an non root account. The following command will create an user and group which is called *pim*.
>
> sudo useradd --create-home -c "pim role account" pim
>
> sudo passwd pim *<password>*

12.1.2 Product 360 - Supplier Portal Default Ports

Port	Protocol	Product 360 Module
9090	http	Product 360 - Supplier Portal (Tomcat Application Server)
25	smtp	Mail Server
8080	http	Product 360 - Media Manager REST
1512	http	Product 360 - Server Service API

If this port is already in use in your installation, follow the instructions below to change the ports:

12.1.2.1 Change Application Server Ports

If you have another application running on your machine which is using the same ports that Product 360 - Supplier Portal uses by default, you may need to change the ports.

To change the ports for Product 360 - Supplier Portal, open the file **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/tomcat/conf/server.xml.**

default server.xml

```
<Server port="9005" shutdown="SHUTDOWN">
...

<Connector port="9090" protocol="org.apache.coyote.http11.Http11NioProtocol"
               connectionTimeout="20000"
               redirectPort="9443"
               URIEncoding="UTF-8" />
```

```

...

<!-- Define an AJP 1.3 Connector on port 9009 -->
<Connector port="9009" protocol="AJP/1.3" redirectPort="9443" />

```

You need to modify the server port (default is 9005), the http nio connector port (default is 9090) and the ajp connector port (default is 9009) to ports that are free on your machine.

> You can use netstat to identify free ports on your machine. See more information on using netstat on Windows.

For example, here are the lines of a modified `server.xml` file, using ports '8005' as server port, '8090' as http nio port and '8009' as ajp connector port:

modified server.xml

```
<Server port="8005" shutdown="SHUTDOWN">
...

<Connector port="8090" protocol="org.apache.coyote.http11.Http11NioProtocol"
               connectionTimeout="20000"
               redirectPort="8443"
               URIEncoding="UTF-8" />

...

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

To access Product 360 - Supplier Portal with this configuration, point your web browser to http://localhost:8090/.

12.2 Supplier Portal Integration

- Prerequisite (see page 146)
- Software Upgrade(10.5.02.01 onwards) (see page 146)
- Setup Product 360 Core Users and Permissions till 10.5.0.02 (see page 146)
  - Create required Users and Groups within Product 360 - Desktop (see page 147)
    - Create Product 360 Supplier Portal Administrator Users Group (see page 147)
    - Create Product 360 - Supplier Portal Item Editor User Group (see page 149)
    - Create Product 360 - Supplier Portal Item Viewer User Group (see page 153)
    - Create Product 360 Supplier Portal System User (see page 156)
    - Add Product 360 Core Users as Product 360 Supplier Portal Administrator (see page 156)

- Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/ Viewer (see page 157)
    - Create Product 360 Supplier Portal Item Editor System User (see page 157)
    - Create Product 360 Supplier Portal Item Viewer System User (see page 157)
- Setup Product 360 Core Users and Permissions starting from 10.5.02.01 (see page 157)
    - Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/ Viewer (see page 158)
    - Create required Users and Groups within Product 360 - Desktop (see page 159)
        - Create Product 360 Supplier Portal Administrator Users Group (see page 159)
        - Create Product 360 - Supplier Portal Item Editor User Group (see page 161)
        - Create Product 360 - Supplier Portal Item Viewer User Group (see page 166)
        - Create Product 360 Supplier Portal System User (see page 169)
        - Add Product 360 Core Users as Product 360 Supplier Portal Administrator (see page 169)
        - Create Product 360 Supplier Portal Item Viewer System User (see page 170)
- Setup communication Product 360 Server - Product 360 Supplier Portal (see page 170)

12.2.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Server Installation
- Desktop Client Installation (see page 95)

12.2.2 Software Upgrade(10.5.02.01 onwards)

Software	Version
Java	17
Tomcat	9.0.82

12.2.3 Setup Product 360 Core Users and Permissions till 10.5.0.02

> Please follow the below steps to set up Product 360 - Supplier Portal Integration, till version 10.5.0.02

There are 3 different kinds of **Product 360 Core Users** for different Product 360 - Supplier Portal use cases:

- **Product 360 Supplier Portal System User**

  - This system user is used to authenticate REST requests at Product 360 - Server which are triggered by suppliers (or Product 360 - Supplier Portal background jobs).

- **Product 360 Supplier Portal Administrator Users**
  - For all actions in Product 360 - Supplier Portal triggered by a portal administrator, the corresponding credentials of the named user are used at the REST interface.

> In order to have an easily maintainable system, it is recommended to create a user group (with the minimal set of common rights) and to assign it to the **Product 360 Supplier Portal System User** and **Product 360 Supplier Portal Administrator Users.**
>
> If object rights are used for an object, please keep in mind that all other users implicitly don't have any rights for it. Thus if an object like a supplier, catalog or mapping shall be used in Product 360 - Supplier Portal context (e.g. for the supplier list, to perform uploads, etc.) the corresponding user group for Product 360 - Supplier Portal **MUST** have full object rights on that object as well.

12.2.3.1 Create required Users and Groups within Product 360 - Desktop

Create Product 360 Supplier Portal Administrator Users Group

- The Product 360 Supplier Portal Users Group needs at least the following action rights to perform the basic actions in Supplier Portal web application:

Rights group	Permission	Mandatory	Note
Catalogs	Supplier catalogs, general access	Yes	
General	Service Login	Yes	
Company Management	Company Management, general access	Yes	
Items	Items, general access	Yes	
Items	Create Items	Yes	
Items	Create Prices	Yes	

Rights group	Permission	Mandatory	Note
Items	Create Prices (in the past)	Yes	
Items	Delete item	Yes	
Items	Delete prices	Yes	
Items	Delete prices (in the past)	Yes	
Items	Edit items	Yes	
Items	Edit prices	Yes	
Items	Edit prices (in the past)	Yes	
Items	View prices	Yes	
Import	Perform import	Yes	
Suppliers	Supplier Management, general access	Yes	
Suppliers	Edit suppliers	Yes	
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	

Rights group	Permission	Mandatory	Note
Users	Users, general access	Yes	

Following **field rights** have to be defined at least as defined below.

Data range	Permission
Partner	As basis grant **visible** and **editable** permissions to all fields. For following fields it is not mandatory to grant permissions: Object rights All fields of the field group Change Information

Create Product 360 - Supplier Portal Item Editor User Group

1. If not already exists, create a new Product 360 Core User Group, which manages the Product 360 Supplier Portal Item Editor permission within Product 360 Core.
2. The Product 360 Supplier Portal Item Editor Users Group needs the following rights:

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Web Permissions	Log in (Web)	Yes	
Web Permissions	Classify objects (Web)	No	
Catalogs	Supplier catalogs, general access	Yes	

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	
Items	Items, general access	Yes	
Items	Edit items	Yes	
Item search	Item search management, general access	Yes	
Products	Product management, general access	Yes	
Products	Edit products	Yes	
Variants	Variant management, general access	Yes	Only in 3 tier product paradigm to classify in structure tree.
Variants	Edit variants	Yes	Only in 3 tier product paradigm to classify in structure tree.
Tasks	Task management, general access	Yes	
Tasks	Edit tasks	No	

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Document management	Document management, general access	No	Only for assignment and upload of media attachments
Document management	Create documents	No	Only for assignment and upload of media attachments
Document management	Create document categories	No	Only for assignment and upload of media attachments
Document management	Edit document categories	No	Only for assignment and upload of media attachments
Multimedia attachments	Add multimedia attachments	No	Only for assignment and upload of media attachments
Merge	Merge, general access	No	
Merge	Perform Merge	No	

Since Product 360 8.1 it is possible to allow the assignment of Supplier Organizations to tasks setup in the system.
The Supplier Organizations that are configured to work with tasks can access them similarly as their general catalog data by the item editor integration.
For this setup at least the field rights for the 'Tasks' data range have to be considered.

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Start date (visible + editable)	Yes	
Tasks	Estimated start date (visible + editable)	Yes	
Tasks	Anticipated completion on (visible + editable)	Yes	
Tasks	Progress (visible + editable)	Yes	
Tasks	Completed on (visible + editable)	Yes	
Item	Item no. (visible + editable)	Yes	
Item	GTIN (visible + editable)	Yes	
Item	Status (visible + editable)	Yes	Field group "Header data"

Interface visibility			
Category	**Name**	**Mandatory**	**Note**
Item	Select the tabs you want to show	optional	

3. Following rights, permissions and interface visibility MUST be REVOKED:

Interface visibility		
Category	**Name**	**Note**
Context	Context visibility: Entire Context selection area	

Action rights		
Rights group	**Permission**	**Note**
Flexible UI	Access Flexible UI	Flex UIs are not supported in context of supplier tasks.

Field rights		
Data range	**Field**	**Note**
Tasks	Revoke all Tasks related field rights NOT listed as mandatory in the previous section.	

> All other Action rights, field rights and all Interface visibility of type 'Web List Definition' and 'Web Tab' not mentioned above have to be defined individuality depending on the scenario and requirements of the project and the individual use case scenarios.
> Here detail tabs, displayed columns and other UI elements needed for the business use case are to be considered.
> For example, if you want to display the short description in the item list view, you have to check the box in the field permissions of the short description for visible.

Create Product 360 - Supplier Portal Item Viewer User Group

1. If not already exists, create a new Product 360 Core User Group, which manages the Product 360 Supplier Portal Item Viewer permission within Product 360 Core.
2. The Product 360 Supplier Portal Item Viewer Users Group needs the following rights:

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Web Permissions	Log in (Web)	Yes	
Catalogs	Supplier catalogs, general access	Yes	
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	
Items	Items, general access	Yes	
Item search	Item search management, general access	Yes	
Products	Product management, general access	Yes	
Variants	Variant management, general access	Yes	Only in 3 tier product paradigm to classify in structure tree.

Since Product 360 8.1 it is possible to allow the assignment of Supplier Organizations to tasks setup in the system.
The Supplier Organizations that are configured to work with tasks can access them similarly as their general catalog data by the item editor integration.
For this setup at least the field rights for the 'Tasks' data range have to be considered.

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Start date (visible)	Yes	

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Estimated start date (visible)	Yes	
Tasks	Anticipated completion on (visible)	Yes	
Tasks	Progress (visible)	Yes	
Tasks	Completed on (visible)	Yes	
Item	Item no. (visible)	Yes	
Item	GTIN (visible)	Yes	
Item	Status (visible)	Yes	Field group "Header data"

Interface visibility			
Category	**Name**	**Mandatory**	**Note**
Item	Select the tabs you want to show	optional	

3. Following permissions, rights and interface visibility MUST be REVOKED:

Interface visibility		
Category	**Name**	**Note**
Context	Context visibility: Entire Context selection area	

Action rights		
Rights group	**Permission**	**Note**
Flexible UI	Access Flexible UI	Flex UIs are not supported in context of supplier tasks.

Field rights		
Data range	**Field**	**Note**
Tasks	Revoke all Tasks related field rights NOT listed as mandatory in the previous section.	

All other Action rights, field rights and all Interface visibility of type 'Web List Definition' and 'Web Tab' not mentioned above have to be defined individuality depending on the scenario and requirements of the project and the individual use case scenarios.
Here detail tabs, displayed columns and other UI elements needed for the business use case are to be considered.
For example, if you want to display the short description in the item list view, you have to check the box in the field permissions of the short description for visible.

Create Product 360 Supplier Portal System User

1. Fill in the user details, keep attention to the following details:
   - the **Active** checkbox must be checked.
   - **Authentication mode** has to be set to **"Internal"**

2. Add User to the created **Product 360 Supplier Portal Administrators User Group**

Add Product 360 Core Users as Product 360 Supplier Portal Administrator

1. Create a new Product 360 Core user or choose an existing Product 360 Core user to add to the Product 360 Supplier Portal Administrator User Group
2. Fill in the user details, keep attention to the following details:

- the **Active** check-box must be checked.
- Add User to the created **Product 360 Supplier Portal Administrators User Group**.

12.2.3.2 Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/Viewer

The item management within Product 360 - Supplier Portal uses the Product 360 - Web functionality. There a two different use cases within Product 360 - Supplier Portal to take into account.

Product 360 Supplier Portal Item Editor:

which means, suppliers are able to edit items within the Product 360 - Supplier Portal.

Product 360 Supplier Portal Item Viewer:

which means, suppliers don't have the ability to edit item data within the Product 360 - Supplier Portal.

> Both users need to be referenced by the webfrontend.properties file of the Product 360 server in order to be used by the system as default system users for Item Editor access through the Supplier Portal.

Create Product 360 Supplier Portal Item Editor System User

1. Fill in the user details, keep attention to the following details:

- the **Active** checkbox must be checked.
- **Authentication mode** has to be set to **"Internal"**

- Add User to the created **Product 360 Supplier Portal Item Editor User Group**.

Create Product 360 Supplier Portal Item Viewer System User

1. Fill in the user details, keep attention to the following details:

- the **Active** checkbox must be checked.
- **Authentication mode** has to be set to **"Internal"**

- Add User to the created **Product 360 Supplier Portal Item Viewer User Group**

12.2.4 Setup Product 360 Core Users and Permissions starting from 10.5.02.01

> Please follow the below steps to set up Product 360 - Supplier Portal Integration, starting from version 10.5.02.01
>
> There will be change in the approach of creating users and user groups for interaction between Product 360 Supplier Portal and Product 360 Core.
>
> There will be no need to create service account users as per the parameters *web.client.hsx.supplier.login* and *web.client.hsx.readonly.supplier.login* from the webfrondend.properties. Having one service account, for all suppliers, would make audit of supplier catalog data in the system irrelevant. Moving forward, there would be a PIM user created for every

Supplier Administrator, Supplier user and Broker user. These users would be auto-assigned to user groups on PIM, based on the access level of the **SUPPLIER** on it's catalogs(provided in P360 Supplier Portal).

There are 3 different kinds of **Product 360 Core Users** for different Product 360 - Supplier Portal use cases:

- **Product 360 Supplier Portal System User**
  - This system user is used to authenticate REST requests at Product 360 - Server which are triggered by suppliers (or Product 360 - Supplier Portal background jobs).
- **Product 360 Supplier Portal Administrator Users**
  - For all actions in Product 360 - Supplier Portal triggered by a portal administrator, the corresponding credentials of the named user are used at the REST interface.

In order to have an easily maintainable system, it is recommended to create a user group (with the minimal set of common rights) and to assign it to the **Product 360 Supplier Portal System User** and **Product 360 Supplier Portal Administrator Users.**

If object rights are used for an object, please keep in mind that all other users implicitly don't have any rights for it. Thus if an object like a supplier, catalog or mapping shall be used in Product 360 - Supplier Portal context (e.g. for the supplier list, to perform uploads, etc.) the corresponding user group for Product 360 - Supplier Portal **MUST** have full object rights on that object as well.

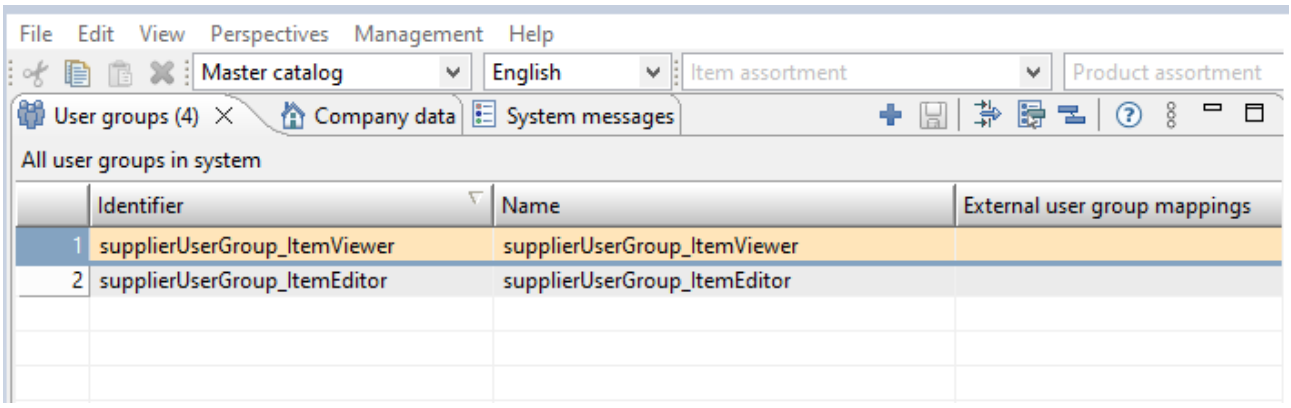
12.2.4.1 Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/Viewer

We will continue to have 2 user groups, one each for Item Viewer and Item Editor. There are new properties added for this purpose in the webfrondend.properties.

Product 360 Supplier Portal Item Editor User Group:
which means, users in this group are able to edit items within the Product 360 - Supplier Portal.
web.client.hsx.itemEditor.userGroup = supplierUserGroup_ItemEditor (default value)

Product 360 Supplier Portal Item Viewer User Group:
which means, users don't have the ability to edit item data within the Product 360 - Supplier Portal.
web.client.hsx.itemViewer.userGroup=supplierUserGroup_ItemViewer (default value)

Please ensure that the user group identifiers for each group and the property values for *web.client.hsx.itemEditor.userGroup* and *web.client.hsx.itemViewer.userGroup* respectively are identical



Default matrix for user group details as per the properties:

Property	Property value	Corresponding user group identifier	Corresponding user group name
web.client.hsx.itemEditor.userGroup	*supplierUserGroup_ItemEditor*	*supplierUserGroup_ItemEditor*	*supplierUserGroup_ItemEditor*
web.client.hsx.itemViewer.userGroup	*supplierUserGroup_ItemViewer*	*supplierUserGroup_ItemViewer*	*supplierUserGroup_ItemViewer*

12.2.4.2 Create required Users and Groups within Product 360 - Desktop

Create Product 360 Supplier Portal Administrator Users Group

- The Product 360 Supplier Portal Users Group needs at least the following action rights to perform the basic actions in Supplier Portal web application:

Rights group	Permission	Mandatory	Note
Catalogs	Supplier catalogs, general access	Yes	
General	Service Login	Yes	

Rights group	Permission	Mandatory	Note
Company Management	Company Management, general access	Yes	
Items	Items, general access	Yes	
Items	Create Items	Yes	
Items	Create Prices	Yes	
Items	Create Prices (in the past)	Yes	
Items	Delete item	Yes	
Items	Delete prices	Yes	
Items	Delete prices (in the past)	Yes	
Items	Edit items	Yes	
Items	Edit prices	Yes	
Items	Edit prices (in the past)	Yes	
Items	View prices	Yes	
Import	Perform import	Yes	

Rights group	Permission	Mandatory	Note
Suppliers	Supplier Management, general access	Yes	
Suppliers	Edit suppliers	Yes	
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	
Users	Users, general access	Yes	
Users	**Create user**	**Yes**	
Users	**Edit user**	**Yes**	

Following **field rights** have to be defined at least as defined below.

Data range	Permission
Partner	As basis grant **visible** and **editable** permissions to all fields. For following fields it is not mandatory to grant permissions: Object rights All fields of the field group Change Information

Create Product 360 - Supplier Portal Item Editor User Group

1. If not already exists, create a new Product 360 Core User Group, which manages the Product 360 Supplier Portal Item Editor permission within Product 360 Core, **assigned** with the following rights.

2. If already exists The Product 360 Supplier Portal Item Editor Users Group need to be **assigned** the extra rights marked in bold:

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Web Permissions	Log in (Web)	Yes	
Web Permissions	Classify objects (Web)	No	
Catalogs	Supplier catalogs, general access	Yes	
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	
Import	**Perform import**	Yes	
Items	Items, general access	Yes	
Items	Edit items	Yes	
Items	**Create items**	Yes	
Item search	Item search management, general access	Yes	
Products	Product management, general access	Yes	
Products	Edit products	Yes	

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Variants	Variant management, general access	Yes	Only in 3 tier product paradigm to classify in structure tree.
Variants	Edit variants	Yes	Only in 3 tier product paradigm to classify in structure tree.
Tasks	Task management, general access	Yes	
Tasks	Edit tasks	No	
Document management	Document management, general access	No	Only for assignment and upload of media attachments
Document management	Create documents	No	Only for assignment and upload of media attachments
Document management	Create document categories	No	Only for assignment and upload of media attachments
Document management	Edit document categories	No	Only for assignment and upload of media attachments

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Multimedia attachments	Add multimedia attachments	No	Only for assignment and upload of media attachments
Merge	Merge, general access	No	
Merge	Perform Merge	No	

Since Product 360 8.1 it is possible to allow the assignment of Supplier Organizations to tasks setup in the system.
The Supplier Organizations that are configured to work with tasks can access them similarly as their general catalog data by the item editor integration.
For this setup at least the field rights for the 'Tasks' data range have to be considered.

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Start date (visible + editable)	Yes	
Tasks	Estimated start date (visible + editable)	Yes	
Tasks	Anticipated completion on (visible + editable)	Yes	
Tasks	Progress (visible + editable)	Yes	
Tasks	Completed on (visible + editable)	Yes	
Item	Item no. (visible + editable)	Yes	

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Item	GTIN (visible + editable)	Yes	
Item	Status (visible + editable)	Yes	Field group "Header data"

Interface visibility			
Category	**Name**	**Mandatory**	**Note**
Item	Select the tabs you want to show	optional	

i. Following rights, permissions and interface visibility MUST be REVOKED:

Interface visibility			
Category	**Type**	**Name**	**Note**
Context		Context visibility: Entire Context selection area	
Action	WebAction	**Action visibility: Import**	To hide the 'Import' action in the Action menu, for the web view that loads in the Supplier portal

Action rights		
Rights group	**Permission**	**Note**
Flexible UI	Access Flexible UI	Flex UIs are not supported in context of supplier tasks.

Field rights		
Data range	**Field**	**Note**
Tasks	Revoke all Tasks related field rights NOT listed as mandatory in the previous section.	

All other Action rights, field rights and all Interface visibility of type 'Web List Definition' and 'Web Tab' not mentioned above have to be defined individuality depending on the scenario and requirements of the project and the individual use case scenarios.
Here detail tabs, displayed columns and other UI elements needed for the business use case are to be considered.
For example, if you want to display the short description in the item list view, you have to check the box in the field permissions of the short description for visible.

Create Product 360 - Supplier Portal Item Viewer User Group

1. If not already exists, create a new Product 360 Core User Group, which manages the Product 360 Supplier Portal Item Viewer permission within Product 360 Core.
2. The Product 360 Supplier Portal Item Viewer Users Group needs the following rights:

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Web Permissions	Log in (Web)	Yes	

Action rights			
Rights group	**Permission**	**Mandatory**	**Note**
Catalogs	Supplier catalogs, general access	Yes	
Structures	Structures, general access	Yes	
Structure groups	Structure groups, general access	Yes	
Items	Items, general access	Yes	
Item search	Item search management, general access	Yes	
Products	Product management, general access	Yes	
Variants	Variant management, general access	Yes	Only in 3 tier product paradigm to classify in structure tree.

Since Product 360 8.1 it is possible to allow the assignment of Supplier Organizations to tasks setup in the system.
The Supplier Organizations that are configured to work with tasks can access them similarly as their general catalog data by the item editor integration.
For this setup at least the field rights for the 'Tasks' data range have to be considered.

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Start date (visible)	Yes	
Tasks	Estimated start date (visible)	Yes	

Field rights			
Data range	**Field**	**Mandatory**	**Note**
Tasks	Anticipated completion on (visible)	Yes	
Tasks	Progress (visible)	Yes	
Tasks	Completed on (visible)	Yes	
Item	Item no. (visible)	Yes	
Item	GTIN (visible)	Yes	
Item	Status (visible)	Yes	Field group "Header data"

Interface visibility			
Category	**Name**	**Mandatory**	**Note**
Item	Select the tabs you want to show	optional	

3. Following permissions, rights and interface visibility MUST be REVOKED:

Interface visibility		
Category	**Name**	**Note**
Context	Context visibility: Entire Context selection area	

Action rights		
Rights group	**Permission**	**Note**
Flexible UI	Access Flexible UI	Flex UIs are not supported in context of supplier tasks.

Field rights		
Data range	**Field**	**Note**
Tasks	Revoke all Tasks related field rights NOT listed as mandatory in the previous section.	

All other Action rights, field rights and all Interface visibility of type 'Web List Definition' and 'Web Tab' not mentioned above have to be defined individuality depending on the scenario and requirements of the project and the individual use case scenarios.
Here detail tabs, displayed columns and other UI elements needed for the business use case are to be considered.
For example, if you want to display the short description in the item list view, you have to check the box in the field permissions of the short description for visible.

Create Product 360 Supplier Portal System User

1. Fill in the user details, keep attention to the following details:
   - the **Active** checkbox must be checked.
   - **Authentication mode** has to be set to **"Internal"**

2. Add User to the created **Product 360 Supplier Portal Administrators User Group**

Add Product 360 Core Users as Product 360 Supplier Portal Administrator

1. Create a new Product 360 Core user or choose an existing Product 360 Core user to add to the Product 360 Supplier Portal Administrator User Group
2. Fill in the user details, keep attention to the following details:

- the **Active** check-box must be checked.
- Add User to the created **Product 360 Supplier Portal Administrators User Group**.

> The user creation and user group assignment is going to be handled by the application, for each supplier administrator, supplier user and supplier broker of each Supplier of Supplier Portal, and hence the explicit steps to create users with 'view-only' and 'edit' options is not needed, any more.

~~**Create Product 360 Supplier Portal Item Editor System User**~~

1. ~~Fill in the user details, keep attention to the following details:~~

- ~~the **Active** checkbox must be checked.~~
- ~~**Authentication mode** has to be set to **"Internal"**~~

- ~~Add User to the created **Product 360 Supplier Portal Item Editor User Group**.~~

~~Create Product 360 Supplier Portal Item Viewer System User~~

1. ~~Fill in the user details, keep attention to the following details:~~

- ~~the **Active** checkbox must be checked.~~
- ~~**Authentication mode** has to be set to **"Internal"**~~

- ~~Add User to the created **Product 360 Supplier Portal Item Viewer User Group**~~

12.2.5 Setup communication Product 360 Server - Product 360 Supplier Portal

There is a possibility to configure the communication between Product 360 Server and Product 360 Supplier Portal. E.g. for Supplier Portal Post Export Step which introduces the possibility for Product 360 Core users to send selected catalog data to a specific supplier within Product 360 Supplier Portal. Or to notify the supplier in the Product 360 Supplier Portal about tasks created for suppliers.

To configure the communication from Product 360 - Server to Product 360 Supplier Portal just make sure you set the following properties in the

<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM\hsx.properties

	Description
`hsx.enabled`	Enable the Product 360 - Server-> Product 360 - Supplier Portal communication `hsx.enabled=true`

`hsx.server`	The Product 360 - Supplier Portal tomcat application server host name. `e.g. hsx.server=localhost`
`hsx.port`	Port of the Product 360 - Supplier Portal application. `e.g. hsx.port=9090`
`hsx.login.name`	`e.g. hsx.login.name=hsx`
`hsx.login.password`	Password of the above portal administrator. `e.g. hsx.login.password=pass` If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
`hsx.rest.uri`	`e.g. hsx.rest.uri=http://localhost:9090/hsx/rest/`
`hsx.suppliertasks.enabled`	Enable tasks for suppliers functionality in the Product 360. Valid values: true and false. Default value: false. Only if both properties hsx.enabled and hsx.suppliertasks.enabled are existing in the configuration file and set to true, the supplier tasks are enabled. `hsx.suppliertasks.enabled=false`
`hsx.suppliertasks.notification.enabled`	Enable notification about created or changed supplier tasks. Valid values: true and false. Default value: false. Only if all properties hsx.enabled, hsx.suppliertasks.enabled and hsx.suppliertasks.notification.enabled are existing in the configuration file and set to true the notifications about supplier tasks will be sent to the timeline of Supplier Portal. `hsx.suppliertasks.notification.enabled=false`

12.3 Media Manager and Supplier Portal Integration

- Prerequisite (see page 172)
- Setup Hotfolder (see page 172)
- Setup REST Service (see page 176)
  - Tomcat and Java (see page 176)
  - Installation HMM REST war (see page 176)
  - Configuration HMM REST war (see page 176)
    - Database configuration (see page 176)
    - Additional configuration (see page 176)
    - Encrypted passwords in configuration files (since 8.0.6.01) (see page 177)
      - Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information (see page 177)
  - Startup (see page 177)

12.3.1 Prerequisite

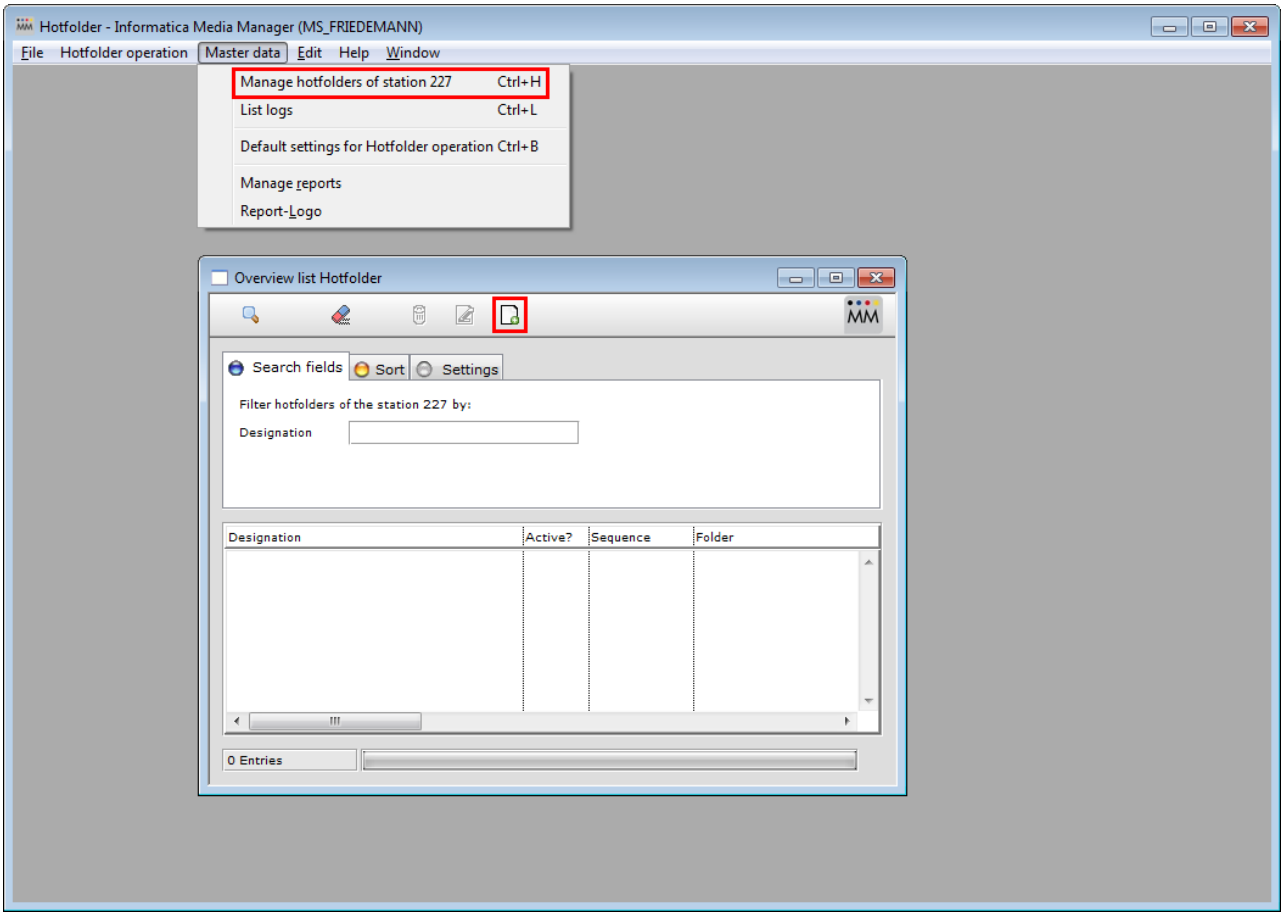
Before you can start with this chapter, you need to have finished the following parts:

- Product 360 - Media Manager Installation (see page 107)

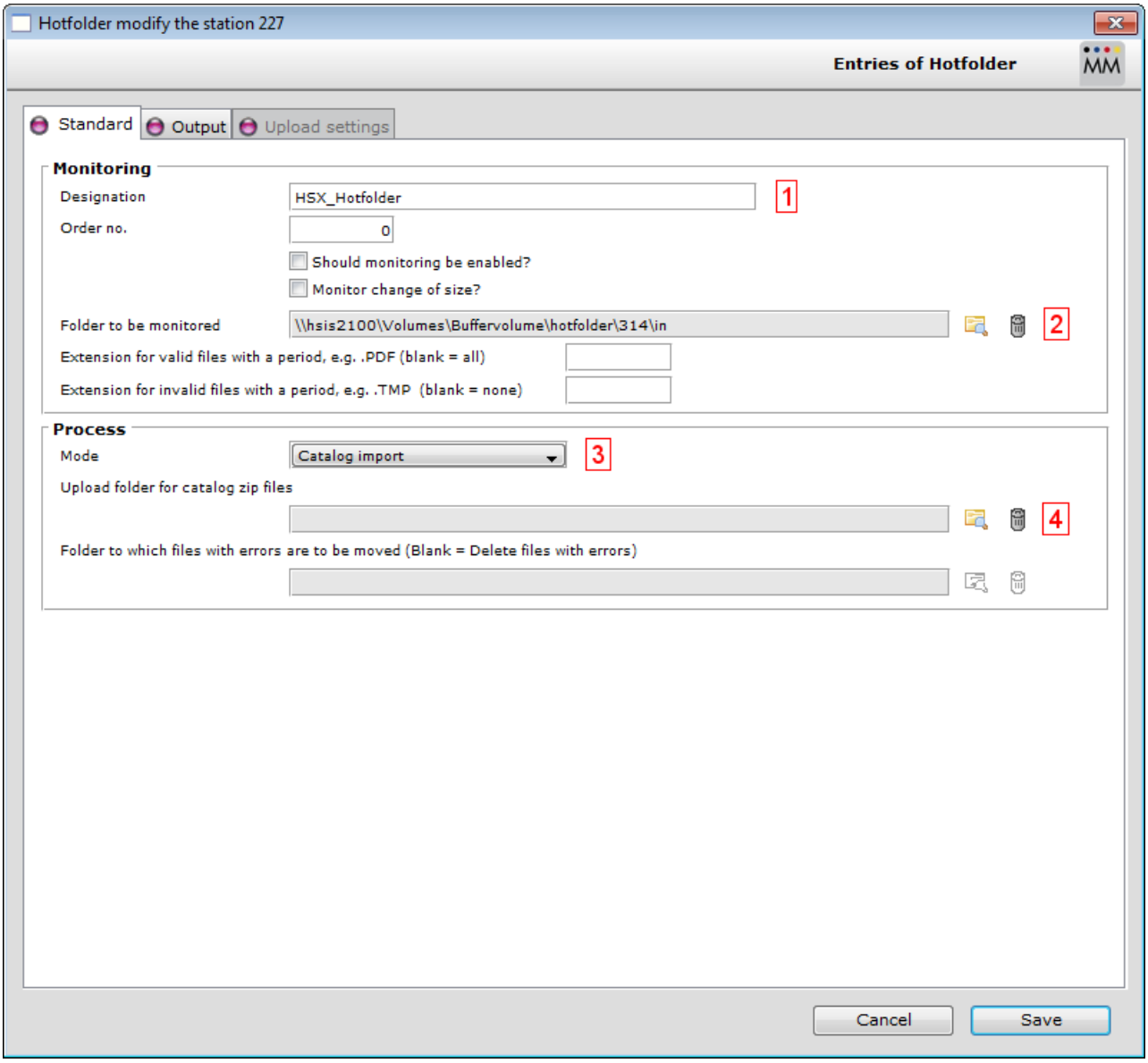
12.3.2 Setup Hotfolder

We have to define a hotfolder in the native Hotfolder client. This hotfolder is monitoring a defined folder and import the found assets to the Product 360 - Media Manager.

Start "administrations mode" of the Hotfolder module.



Choose "Manage hotfolder of station XX" and create a new Hotfolder defintion.



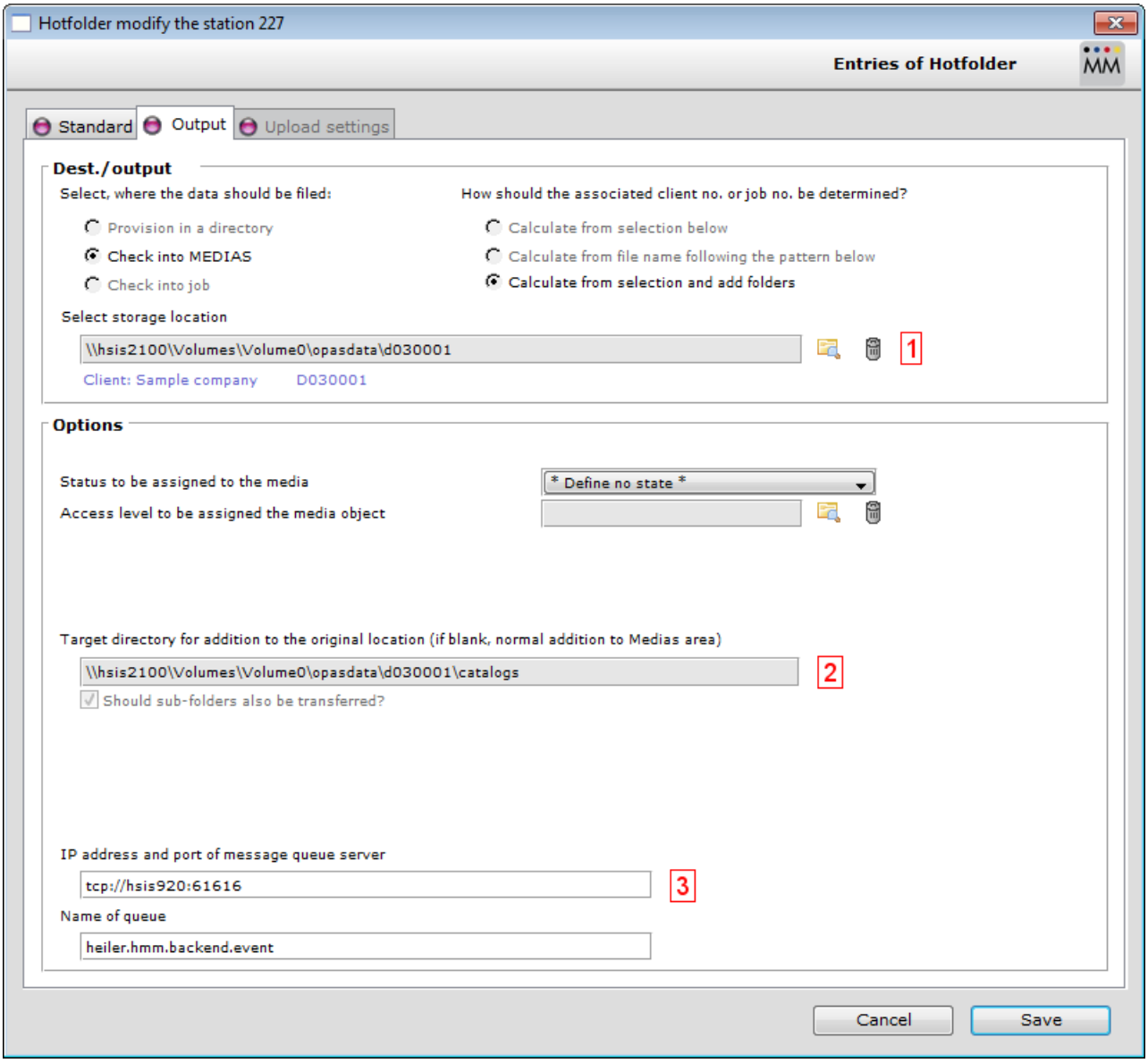
Settings at the Standard panel:

#1: Define a name for the Hotfolder

#2: Select a folder to be monitored.

#3: Define mode "Catalog import".

#4: Choose a target folder for the uncompressed uploads



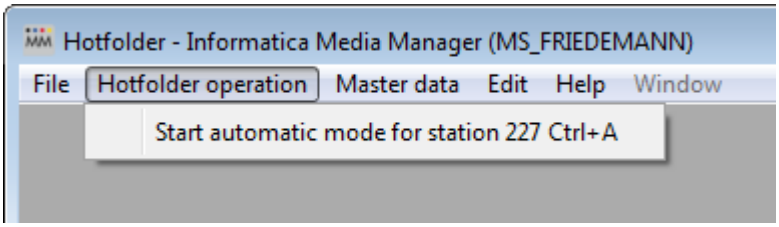
Additional settings are defined at the "Output" panel.

#1: Choose a customer. This customer has to be defined be the REST service configuration.

#2: Check if the folder exists. If not create the "catalogs" folder.

#3: Define the location of your ActiveMQ and enter the name of the queue. Default name is "heiler.hmm.backend.event".

The configuration is done now. Save your settings ...



... and start the Hotfolder.

12.3.3 Setup REST Service

Now we have to setup the REST service to upload the asset containing archives. Due to performance reasons we recommended to use different machines for the REST service and the Hotfolder.

12.3.3.1 Tomcat and Java

It is recommended to use the Tomcat included in the OpasGWebserver.zip of the Media Manager Web application.

12.3.3.2 Installation HMM REST war

Add the HMM REST war to the tomcat by copying the rest.war file to Tomcat/webapps/ folder.

12.3.3.3 Configuration HMM REST war

The REST service has to be configured. The config files can be found at Tomcat/webapps/rest/WEB-INF/classes/META-INF/spring

Database configuration

Configure your HMM database at the file hmm-database.properties. This connection is the same connection used by the native HMM modules. A connection could look like this:

```
database.type=oracle
database.url=jdbc:oracle:thin:@hsis300:1521:hmm
database.username=opasuser
database.password=OPASPASS
database.driverClassName=oracle.jdbc.driver.OracleDriver
```

Additional configuration

Configure the HMM customer in the config file hmm-inbox.properties . The customer number has to be defined at the key hmm.inbox.standardOrganisation

Encrypted passwords in configuration files (since 8.0.6.01)

Product 360 Media Manager Web supports the encryption of secure information like passwords in the configuration files. The encryption will be executed only if your secure information in the configuration files is enclosed by the marker `[_to_encrypt_]`.
So, if you want to have e.g. the password "Password" encrypted in a configuration file just use the marker before and after the password like this: `[_to_encrypt_]Password[_to_encrypt_]`. Please note first encryption gets done with the start of the Tomcat.

For example in `hmm-database.properties`:

properties file

```
database.type=mssql
database.url=jdbc:sqlserver://host:1433;DatabaseName=dbname
database.username=user
database.password=[_to_encrypt_]Password[_to_encrypt_]
database.driverClassName=com.microsoft.sqlserver.jdbc.SQLServerDriver
```

Usage of strong cryptographic algorithms to encrypt/decrypt secure information

Due to import control restrictions of some countries, the version of the JCE policy files that are bundled in the Java 8 Runtime Environment allow "strong" but limited cryptography to be used. This means if you want to use a strong cryptographic algorithm like AES-256 you will need to replace your Java Runtime's JCE policy files in the `OpasGWebServer\java\jre\lib\security` folder. Otherwise you will run into errors during encryption/decryption in Product 360 Media Manager Web, saying you're using an illegal key size.
Also after update to newest Hotfix the Java JCE policy files must be replaced in corresponding `OpasGWebServer\java\jre\lib\security` folder.

See also http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information

Product 360 Media Manager Rest Service provides a default implementation for the encryption of secure information with an internal and securely stored Key using AES-256.
For sophisticated deployments we recommend to integrate with Encryption Key Management solutions like Amazon AWS or Azure KeyVault and use the API we offer to send and receive data for encryption to these key stores securely.

12.3.3.4 Startup

Start your Tomcat. The default URL of the REST service is

YOUR_MASCHINE:YOUR_TOMCAT_PORT/rest/rest

Check HSX Functions and Installation for additional information about the existing REST calls.

12.4 Web and Supplier Portal Integration

12.4.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Server Installation

12.4.2 Configure Product 360 Supplier Portal Item Editor System User within Product 360 - Web

Navigate to your Product 360 - Server Installation root and configure the following Product 360 - Web Configuration File:

<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM\webfrontend.properties

Make sure to configure the following properties:

Database Settings	
`web.client.hsx.supplier.login`	Product 360 Supplier Portal Item Editor System User `e.g. web.client.hsx.supplier.login=supplier`
`web.client.hsx.supplier.password`	Product 360 Supplier Portal Item Editor System User password If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
`web.client.hsx.readonly.supplier.login`	Product 360 Supplier Portal Item Viewer System User `e.g. web.client.hsx.readonly.supplier.login=readonlysupplier`

`web.client.hsx.readonly.supplier.password`	Product 360 Supplier Portal Item Viewer System User password If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.

12.5 Server Installation on Windows

- Prerequisite (see page 179)
- Download the Product 360 Supplier Portal zip (see page 179)
- Create Your Product 360 Supplier Portal Server Installation Root (see page 180)
- Configuration (see page 180)
  - Configure Product 360 Supplier Portal central configuration file (see page 180)
    - Setup Database Connection (see page 180)
      - Database Settings (see page 181)
    - Setup Product 360 - Server Connection (see page 182)
      - HPM Settings (see page 182)
    - Setup Product 360 - Media Manager Connection (see page 182)
      - HMM Settings (see page 183)
    - Setup Mail Server (see page 183)
      - Mail Server Settings (see page 183)
    - Setup File Storage Location (see page 184)
      - FileStorage Settings (see page 184)
    - Setup Product 360 - Supplier Portal URL Root (see page 184)
  - Configure Logging (see page 185)
- Install Tomcat (see page 185)
  - Install Product 360 - Supplier Portal Tomcat Windows Service (see page 185)
  - Start/Stop/Configure Product 360 - Supplier Portal Tomcat Windows Service (see page 186)
  - (optional) Uninstall Product 360 - Supplier Portal Tomcat Windows Service (see page 187)

12.5.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Setup Product 360 - Supplier Portal Database (see page 66)
- Product 360 Core and Supplier Portal Integration (see page 145)
- Product 360 - Media Manager and Supplier Portal Integration (see page 172)
- Product 360 - Web and Supplier Portal Integration (see page 178)

12.5.2 Download the Product 360 Supplier Portal zip

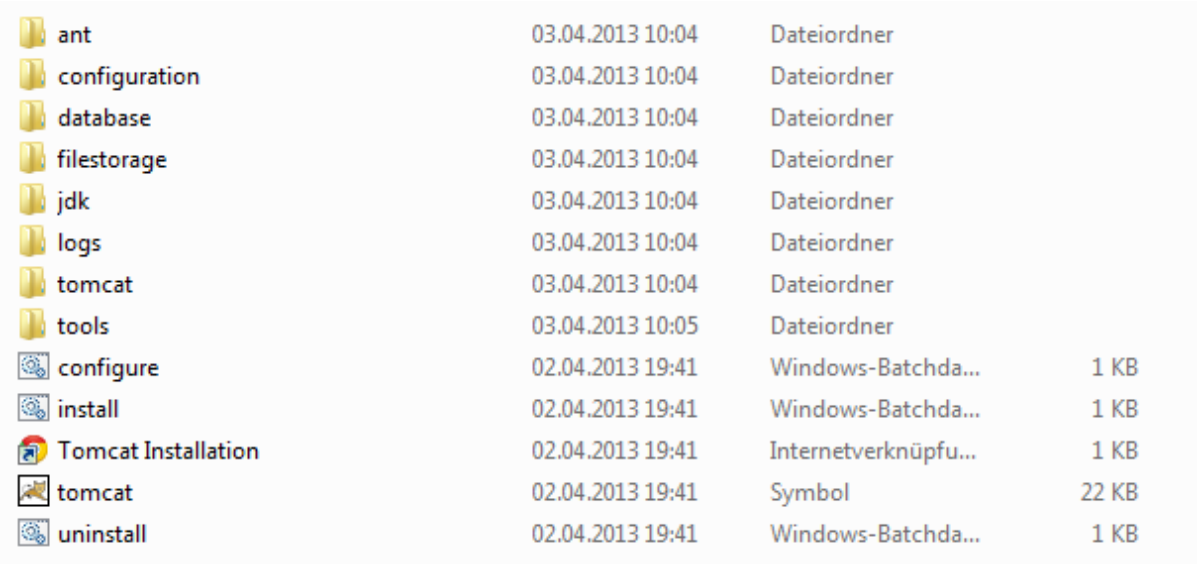
To obtain the download package for Product 360 Supplier Portal please raise a Shipping Request with Informatica.

12.5.3 Create Your Product 360 Supplier Portal Server Installation Root

1. In case you don't use same location like in your database installation, you have to unzip/copy the PIM_<*Version*>_SupplierPortal.zip again to the new location.
2. In this manual we assume you are using the following installation root:

   <INSTALLATION ROOT> = *C:\INFORMATICA\PIM\SupplierPortal*
   feel free to change this to another location.

   Screenshot: Product 360 - Supplier Portal Folder Structure



ant	03.04.2013 10:04	Dateiordner	
configuration	03.04.2013 10:04	Dateiordner	
database	03.04.2013 10:04	Dateiordner	
filestorage	03.04.2013 10:04	Dateiordner	
jdk	03.04.2013 10:04	Dateiordner	
logs	03.04.2013 10:04	Dateiordner	
tomcat	03.04.2013 10:04	Dateiordner	
tools	03.04.2013 10:05	Dateiordner	
configure	02.04.2013 19:41	Windows-Batchda...	1 KB
install	02.04.2013 19:41	Windows-Batchda...	1 KB
Tomcat Installation	02.04.2013 19:41	Internetverknüpfu...	1 KB
tomcat	02.04.2013 19:41	Symbol	22 KB
uninstall	02.04.2013 19:41	Windows-Batchda...	1 KB

12.5.4 Configuration

Before running the Product 360 Supplier Portal application server, some basic configuration needs to be done.

12.5.4.1 Configure Product 360 Supplier Portal central configuration file

All configuration properties can be found under the location: **<INSTALLATION ROOT>/configuration/configuration.properties**. See the Configuration Manual for more information about all possible configuration parameters. For a default installation the following aspects need special attention:

Setup Database Connection

Make sure you set the following database properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

Database Settings	
`database.type`	Type of DBMS `mssql/oracle`

`database.name`	MSSQL: Name of the created database
	`e.g. database.name=hsx_1.4`
	Oracle: SID or ServiceName of the Oracle DB
	`e.g. database.name=XE`

`database.server`	Hostname of the database server `e.g. database.server=localhost`
`database.port`	Port number of the database server `e.g. MSSQL default is database.port=1433` If you want to connect P360 Supplier Portal to an Oracle Database via TCPS, please refer to chapter "How to configure a secure database connection for Product 360 Supplier Portal" in the "Supplier Portal Configuration" manual.
`database.username`	database user you created while setup the database. `e.g. database.username=hsx`
`database.password`	password for the above specified database user If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.

The installation zip also comes with a Hibernate configuration file (**<INSTALLATION ROOT>/configuration/persistence-[DBMS].xml**) for each supported DBMS. Be careful when changing values in these files, usually this is not needed.

Setup Product 360 - Server Connection

All communication between Product 360 Supplier Portal and Product 360 - Server is done using REST, which means via HTTP. No direct access to the Product 360 Core database or specific Product 360 - Server directories is needed. The Product 360 - Server Service API is protected via HTTP authentication.

Make sure you set the following Product 360 - Server properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

HPM Settings	

`hpm.restUri`	`Product 360 - Server Service API Base URL`
	
	`e.g. hpm.restUri=http://localhost:1512/rest`

`hpm.webClientUri`	`Product 360 - Web URL`
	
	`e.g. http://localhost:1512/pim/webaccess`

`hpm.systemUserName`	Product 360 Core User --> Product 360 Supplier Portal System User `e.g. hpm.systemUserName=hsx`
`hpm.systemUserPassword`	Product 360 Supplier Portal System User's password If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.

You can test the configured Product 360 - Server/Product 360 Supplier Portal connection in the browser by entering the REST URL and providing the given user credentials. Example: localhost:1501/rest/V1.0/list/info

Setup Product 360 - Media Manager Connection

Make sure you set the following hmm properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

HMM Settings	

`hmm.restUri`	`Product 360 – Media Manager REST Services URL`
	
	`e.g. hmm.restUri=http://hmmserver:8080/rest/rest`

Similar to Product 360 - Server/Product 360 Supplier Portal the communication is done via REST. The Product 360 - Media Manager REST interface is not protected at all so make sure that it is visible internally only.

Setup Mail Server

Make sure you set the following mail server properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

Mail Server Settings	
`mail.enabled`	To activate mail notification within Product 360 - Supplier Portal set this property to true. `mail.enabled=true`
`mail.protocol`	Mail protocol as passed to javax.mail `e.g. mail.protocol=smtp`
`mail.serverHost`	Mail server host `e.g. mail.serverHost=smtp.company.com`
`mail.serverPort`	Mail server port `e.g. mail.serverPort=25`
`mail.senderAddressDefault`	The default sender address for mails. Will be used and displayed as mail sender. `e.g. admin@company.com`

`mail.username`	User for mail server authentication. (only in case your mail server requires authentication)
`mail.password`	User password for mail server authentication. If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.

Setup File Storage Location

Product 360 - Supplier Portal also stores binary files (e.g. files uploaded to the timeline or used for test runs). These files are not stored in the database but in the file system. The location needs to be configured, too. This could also be a Windows shared drive.

Make sure you set the following file storage property in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

FileStorage Settings	
`fileStorageService.rootDirectory`	Folder pointing to the root directory for all binary files `e.g C:/HEILER/HSX/filestorage`

Setup Product 360 - Supplier Portal URL Root

Make sure you set the following URL root property in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

URL Root Settings	
`hostAdressWithAppRoot`	Product 360 Supplier Portal Root Url. Normally contains the absolute path including context path plus the suffix "/html/" `e.g. hostAdressWithAppRoot=http://localhost:9090/hsx/html/`

12.5.4.2 Configure Logging

Product 360 Supplier Portal uses Logback (successor of log4j) as logging framework. The logging configuration can be defined *at* **<INSTALLATION ROOT>/configuration/logback.xml**.

By default, the log files are written to **C:\Heiler\HSX\logs**. If your installation root vary from this location you have to fix all occurrences in the logging configuration file **<INSTALLATION ROOT>/configuration/logback.xml**.

Screenshot: Cutout of the logging configuration file

```
1   <?xml version="1.0" encoding="UTF-8"?>
2   <configuration>
3       <!-- Logger configuration for the HSX production environment. Log file must
4           be activated using -Dlogback.configurationFile=logback-prod.xml -->
5
6       <contextListener class="ch.qos.logback.classic.jul.LevelChangePropagator" />
7
8       <appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
9           <file>C:/HEILER/HSX/logs/hsx.log</file>
10          <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
11              <!-- daily rollover -->
12              <fileNamePattern>C:/HEILER/HSX/logs/hsx.%d{yyyy-MM-dd}-%i.log.zip</fileNamePattern>
13
14              <timeBasedFileNamingAndTriggeringPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedFNATP">
15                  <!-- or whenever the file size reaches 50MB -->
16                  <maxFileSize>50MB</maxFileSize>
17              </timeBasedFileNamingAndTriggeringPolicy>
18
19              <!-- keep 10 days' worth of history -->
20              <maxHistory>10</maxHistory>
21          </rollingPolicy>
22
23          <encoder>
24              <pattern>%d{MM/dd HH:mm:ss.SSS} [%thread] [%X{user}] %-3level %logger{36} - %msg%n</pattern>
25          </encoder>
26      </appender>
27
28      <appender name="PERFORMANCE_FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
29          <file>C:/HEILER/HSX/logs/hsx_performance.log</file>
30          <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
```

12.5.5 Install Tomcat

A pre-configured Apache Tomcat is part of the Product 360 - Supplier Portal archive and can be found in the directory **<INSTALLATION ROOT>/tomcat**. It is recommended to run Product 360 - Supplier Portal Tomcat as a Windows Service.

12.5.5.1 Install Product 360 - Supplier Portal Tomcat Windows Service

The installation root contains three batch files to install (*install.bat*) and uninstall (*uninstall.bat*) and configure (*configure.bat*) the Tomcat service.

1. Open a new command line **with administrator privileges** (choose "**Run as administrator**" in context menu)
2. Navigate into the **<INSTALLATION ROOT>**

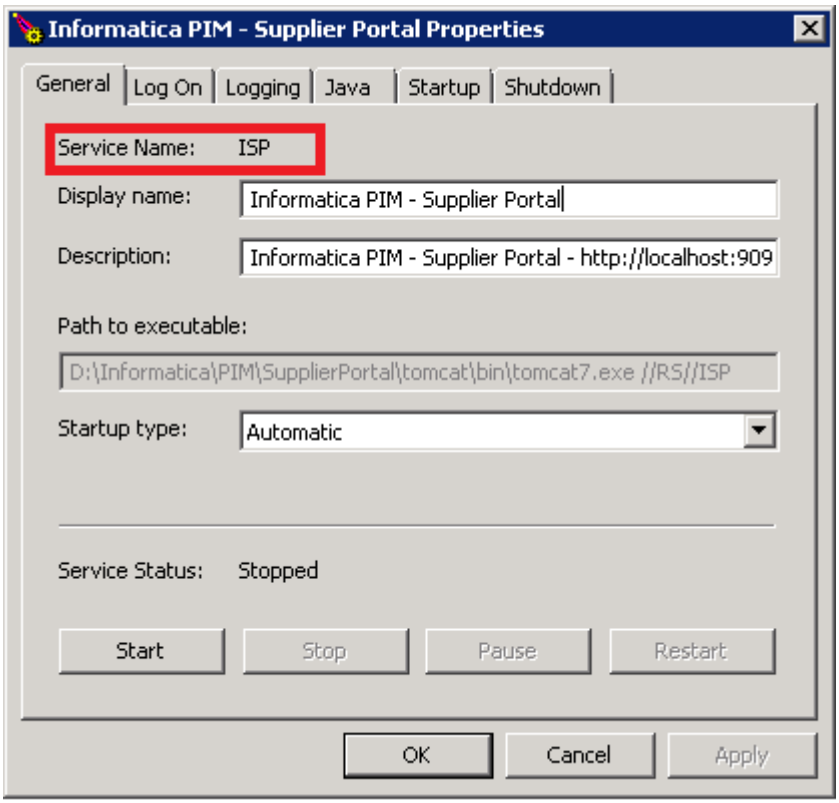
3. To install the tomcat with the default service name **Supplier Portal**, run the batch file **<INSTALLATION ROOT>/install.bat** to register the Tomcat Windows Service. If you wish to define a different service name, run the batch file with the desired new service name as argument: **<INSTALLATION ROOT>/install.bat ServiceName**

12.5.5.2 Start/Stop/Configure Product 360 - Supplier Portal Tomcat Windows Service

> You need to install the service before you can configure it.

Run the file **<INSTALLATION ROOT>configure.bat**. If you installed the service under an different service name, then the default **ISP**, you have to run the configure batch file with your service name as argument: **<INSTALLATION ROOT>/configure.bat ServiceName**

To initially start Tomcat, open the General Tab and press **Start.**



By default, Tomcat runs on port **9090**. No SSL is configured. No Tomcat user is configured for the Tomcat manager application. To change any of the Tomcat settings, edit the configuration files in **<INSTALLATION ROOT>/tomcat/conf**. See the Tomcat manual for more information.

The Product 360 - Supplier Portal application server is deployed within the **<INSTALLATION ROOT>/tomcat/webapps** directory. The default name is **hsx.war** that means that the default local URL is ***http://localhost:9090/hsx***. To change the URL suffix, rename the war file accordingly.

After Tomcat has been registered successfully, it is automatically started. The war file in the **webapps** folder is deployed and the application starts. To verify that everything works as expected open *http://localhost:9090/hsx* in a browser. Go to the login page and log in with any existing Product 360 Core user to act as a portal administrator.

12.5.5.3 (optional) Uninstall Product 360 - Supplier Portal Tomcat Windows Service

The installation root contains three batch files to install (*install.bat*) and uninstall (*uninstall.bat*) and configure (*configure.bat*) the Tomcat service.

1. Open a new command line **with administrator privileges** (choose "**Run as administrator**" in context menu)
2. Navigate into the **<INSTALLATION ROOT>**
3. To uninstall the tomcat with the default service name **ISP**, run the batch file **<INSTALLATION ROOT>/uninstall.bat** to unregister the Tomcat Windows Service. If you installed the service under an different service name then the default **ISP**, you have to run the uninstall batch file with your service name as argument: **<INSTALLATION ROOT>/uninstall.bat ServiceName**

If you want to connect P360 Supplier Portal to an Oracle Database via TCPS, please refer to chapter "How to configure Oracle TCPS connection for P360 Supplier Portal" in the "Supplier Portal Configuration" manual.

12.6 Server Installation on Linux

12.6.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Supplier Portal Database
- Supplier Portal Integration
- Media Manager and Supplier Portal Integration
- Web and Supplier Portal Integration

> You will need root privileges to install the supplier portal on your system.

12.6.1.1 Java

Please ensure that the suitable Java JRE is used for running Supplier Portal.
Use the JRE

- that is located in the jre-linux folder of the Supplier Portal package (see below how to get that)
- that is already part of the Product 360 Core suite,
- or download it for your Linux distribution

If you're not sure whether you have Java installed correctly:

> ⚠ *** Java 17 required for Product 360 v.10.5.0.01.00 and above*

1. Open a terminal.
2. Type in the following command:

```
echo $JAVA_HOME
```

3. Result
   a. If there is a path displayed such as `/opt/jdk17` , then Java is installed and properly configured.
   b. If nothing is displayed, then you either need to install Java or set the `$JAVA_HOME` environment variable. You can set this environment variable in your user account's ''~.profile" or system-wide in "/etc/profile". In case of an service user without an linked shell you need to set the JAVA_HOME within the supplier portals wrapper.conf.

12.6.2 Download the Product 360 Supplier Portal zip

To obtain the download package for Product 360 Supplier Portal please raise a Shipping Request with Informatica.

12.6.3 Create Your Product 360 Supplier Portal Server Installation Root

1. In case you don't use same location like in your database installation, you have to unzip/copy the PIM_<*Version*>_SupplierPortal.zip again to the new location.

```
sudo mkdir <INSTALL ROOT>
sudo unzip hsx.zip -d <INSTALL ROOT>
```

2. In this manual we assume you are using the following installation root:
   <INSTALLATION ROOT> = /opt/pim/*supplierPortal*
   feel free to change this to another location.

12.6.4 Configuration

Before running the Product 360 Supplier Portal application server, some basic configuration needs to be done.

12.6.4.1 Configure Product 360 Supplier Portal central configuration file

All configuration properties can be found under the location: **<INSTALLATION ROOT> /configuration/configuration.properties**. See the Configuration Manual for more information about all possible configuration parameters. For a default installation the following aspects need special attention:

Setup Database Connection

Make sure you set the following database properties in the **<INSTALLATION ROOT> /configuration/ configuration.properties** file.

Database Settings	
`database.type`	Type of DBMS `mssql/oracle`

`database.name`	MSSQL: Name of the created database
	`e.g. database.name=hsx_1.4`
	Oracle: SID or ServiceName of the Oracle DB
	`e.g. database.name=XE`

`database.server`	Hostname of the database server `e.g. database.server=localhost`
`database.port`	Port number of the database server `e.g. MSSQL defaul is database.port=1433` If you want to connect P360 Supplier Portal to an Oracle Database via TCPS, please refer to chapter "How to configure a secure database connection for Product 360 Supplier Portal" in the "Supplier Portal Configuration" manual.
`database.username`	database user you created while setup the database. `e.g. database.username=hsx`
`database.password`	password for the above specified database user

The installation zip also comes with a Hibernate configuration file (**<INSTALLATION ROOT> /configuration/persistence-[DBMS].xml**) for each supported DBMS. Be careful when changing values in these files, usually this is not needed.

Setup Product 360 - Server Connection

All communication between Product 360 Supplier Portal and Product 360 - Server is done using REST, which means via HTTP. No direct access to the Product 360 Core database or specific Product 360 - Server directories is needed. The Product 360 - Server Service API is protected via HTTP authentication.

Make sure you set the following Product 360 - Server properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

HPM Settings	
`hpm.restUri`	`Product 360 - Server Service API Base URL` `e.g. hpm.restUri=http://localhost:1501/rest`
`hpm.webClientUri`	`Product 360 - Web URL` `e.g. http://localhost:1501/pim/webaccess`
`hpm.systemUserName`	Product 360 Core User --> Product 360 Supplier Portal System User `e.g. hpm.systemUserName=hsx`
`hpm.systemUserPassword`	Product 360 Supplier Portal System User's password

You can test the configured Product 360 - Server/Product 360 Supplier Portal connection in the browser by entering the REST URL and providing the given user credentials. Example: localhost:1501/rest/V1.0/list/info

Setup Product 360 - Media Manager Connection

Make sure you set the following hmm properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

HMM Settings	

`hmm.restUri`	`Product 360 - Media Manager REST Services URL`
	
	`e.g. hmm.restUri=http://hmmserver:8080/rest/rest`

Similar to Product 360 - Server/Product 360 Supplier Portal the communication is done via REST. The Product 360 - Media Manager REST interface is not protected at all so make sure that it is visible internally only.

Setup Mail Server

Make sure you set the following mail server properties in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

Mail Server Settings	
`mail.enabled`	To activate mail notification within Product 360 - Supplier Portal set this property to true. `mail.enabled=true`
`mail.protocol`	Mail protocol as passed to javax.mail `e.g. mail.protocol=smtp`
`mail.serverHost`	Mail server host `e.g. mail.serverHost=smtp.company.com`
`mail.serverPort`	Mail server port `e.g. mail.serverPort=25`
`mail.senderAddressDefault`	The default sender address for mails. Will be used and displayed as mail sender. `e.g. admin@company.com`

`mail.username`	User for mail server authentication. (only in case your mail server requires authentication)
`mail.password`	User password for mail server authentication.

Setup File Storage Location

Product 360 - Supplier Portal also stores binary files (e.g. files uploaded to the timeline or used for test runs). These files are not stored in the database but in the file system. The location needs to be configured, too.

Make sure you set the following file storage property in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

FileStorage Settings	
`fileStorageService.rootDirectory`	Folder pointing to the root directory for all binary files `e.g /opt/pim/supplierPortal/filestorage`

Setup Product 360 - Supplier Portal URL Root

Make sure you set the following URL root property in the **<INSTALLATION ROOT>/configuration/configuration.properties** file.

URL Root Settings	
`hostAdressWithAppRoot`	Product 360 Supplier Portal Root Url. Normally contains the absolute path including context path plus the suffix "/html/" `e.g. hostAdressWithAppRoot=http://localhost:9090/hsx/html/`

12.6.4.2 Configure Logging

Product 360 Supplier Portal uses Logback (successor of log4j) as logging framework. The logging configuration can be defined *at* **<INSTALLATION ROOT>/configuration/logback.xml**.

> ⚠ By default the log configuration is using windows path **C:\ Heiler \ HSX\logs** definitions so you need to change them to an unix path e.g. **/opt/pim/supplierPortal/logs**. Fix all occurrences in the logging configuration file **<INSTALLATION ROOT>/configuration/logback.xml**.

Screenshot: Cutout of the logging configuration file

```
1   <?xml version="1.0" encoding="UTF-8"?>
2   <configuration>
3       <!-- Logger configuration for the HSX production environment. Log file must
4           be activated using -Dlogback.configurationFile=logback-prod.xml -->
5
6       <contextListener class="ch.qos.logback.classic.jul.LevelChangePropagator" />
7
8       <appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
9           <file>C:/HEILER/HSX/logs/hsx.log</file>
10          <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
11              <!-- daily rollover -->
12              <fileNamePattern>C:/HEILER/HSX/logs/hsx.%d{yyyy-MM-dd}-%i.log.zip</fileNamePattern>
13
14              <timeBasedFileNamingAndTriggeringPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedFNATP">
15                  <!-- or whenever the file size reaches 50MB -->
16                  <maxFileSize>50MB</maxFileSize>
17              </timeBasedFileNamingAndTriggeringPolicy>
18
19              <!-- keep 10 days' worth of history -->
20              <maxHistory>10</maxHistory>
21          </rollingPolicy>
22
23          <encoder>
24              <pattern>%d{MM/dd HH:mm:ss.SSS} [%thread] [%X{user}] %-3level %logger{36} - %msg%n</pattern>
25          </encoder>
26      </appender>
27
28      <appender name="PERFORMANCE_FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
29          <file>C:/HEILER/HSX/logs/hsx_performance.log</file>
30          <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
```

12.6.5 Install Tomcat

A pre-configured Apache Tomcat is part of the Product 360 - Supplier Portal archive and can be found in the directory **<INSTALLATION ROOT>/ tomcat**. It is recommended to run Product 360 - Supplier Portal Tomcat as an service.

> We recommand to create an service user to run the tomcat under an non root account. The following command will create an user and group which is called *pim*.
>
> sudo useradd --create-home -c "pim role account" pim
>
> sudo passwd pim *<password>*

12.6.5.1 Install Product 360 - Supplier Portal Tomcat Linux Service

The installation root contains one shell script (*pimsupplierportal.sh*) to install, remove, start, stop and get status information.

1. Open a terminal
2. Change ownership of install root to service user and group *pim*

```
sudo chown -R pim:pim /opt/pim/supplierPortal
```

3. Change file and directory permissions

```
sudo chmod -R 755 /opt/pim/supplierPortal
```

4. (Optional) In case your servcie user is an system user with no linked shell you have to set the JAVA_HOME variable directly within supplier portal configuration wrapper.conf.
   a. Go to the tomcat configuration directory and edit the wrapper configuration file **<INSTALLATION ROOT>/ tomcat/conf/wrapper.conf**.
   wrapper.java.command=/home/username/java/jdk17/bin/java

5. Install the server by executing the **<INSTALLATION ROOT>/pimsupplierportal.sh** script as root.

```
cd /opt/pim/supplierPortal
sudo ./pimsupplierportal.sh install
```

12.6.5.2 Start/Stop Supplier Portal Tomcat Server

You can use the **<INSTALLATION ROOT>/pimsupplierportal.sh** script to start/stop the tomcat server with the Supplier Portal using the service user account.

```
su pim
cd /opt/pim/supplierPortal

# to start the Supplier Portal
./pimsupplierportal.sh start

# to stop the Supplier Portal
./pimsupplierportal.sh stop

# get current service status
./pimsupplierportal.sh status
```

12.6.5.3 Deinstallation

```
cd /opt/pim/supplierPortal
sudo ./pimsupplierportal.sh remove
```

12.7 Language Pack Installation

12.7.1 Overview

This page describes how to install an additional language pack for Product 360 Supplier Portal. The language pack is part of the official release package since version 7.1.02. For earlier versions, the package is available on request from Product Management Team / R&D.

12.7.2 Installation

- Open the folder <INSTALL_DIRECTORY>/configuration/i18n on the Product 360 Supplier Portal Server
- Unzip the language pack file SupplierPortal_LanguagePack.zip into that folder
    - Please not that the language pack contains all language files, including German and English
    - Please make sure to backup the old content in of modifications have been made to these files
- Open /configuration/server.properties file and check the settings i18n.uiResourcesPath and i18n.serverResourcesPath. The values should look like this:

```
i18n.uiResourcesPath=file:${hsx.configurationArea}/i18n/ui/**/*Messages.properties
i18n.serverResourcesPath=file:${hsx.configurationArea}/i18n/server/**/
*Messages.properties
```

- Check the property *i18n.availableUiLocales* and make sure all desired locales are listed. This property can be used to provide only a subset of all licensed languages within Supplier Portal.
- Restart Product 360 Supplier Portal Tomcat Service

Users can select their UI language on the login page. Only languages are displayed that are covered by a corresponding Product 360 license module in the Product 360 Application Server.

12.8 Installation Troubleshooting

In case the application doesn't work as expected, you might try the following:

Problem	Possible solution
The Tomcat service registration fails with an error.	• Make sure to run the service registration **as local administrator**. • Make sure no other Tomcat with the same service name is already installed. • Don't use blanks in the Tomcat service name.

Problem	Possible solution
Tomcat doesn't start.	• Take a look at the Tomcat log files in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/tomcat/logs** • Make sure that the configured ports are not in use. You can change the ports in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/tomcat/conf/server.xml.** • Depending on the local configuration, Tomcat might not have sufficient rights to open ports. Run the Tomcat service as an appropriate user in this case. • Make sure to use the right JDK for Tomcat. You can set the JDK using the Windows Tomcat service by opening the file **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/configure.bat**. Choose the tab **Java** and check the JVM Settings: • The path of the **Java Virtual Machine (JVM)** entry should be: **<jdk_home_dir>\jre\bin\server\jvm.dll**. Make sure that you use a **64 bit Java version**.

Problem	Possible solution
Tomcat starts but the webapp doesn't.	• Take a look at the Product 360 - Supplier Portal log files in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/logs** or at Tomcat log files in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/tomcat/logs** • Test the database connection. • Check if the database tables have been created. If not, run the script again and look for errors. • Test the Product 360 - Server connection. Product 360 - Supplier Portal doesn't start if Product 360 - Server cannot be reached. If Product 360 - Server runs but Product 360 - Supplier Portal reports an error, take a look at the Product 360 - Server logs. • Make sure that the **configuration.properties** file and its properties are valid. **Please keep in mind**, that every '**properties'** file (ending with ***.properties**) will be read and all contained properties will be imported (e.g. if you have a copy of the **configuration.properties** file which also ends with ***.properties** and its properties are changed, this could lead to unpredictable property values of the Product 360 - Supplier Portal system). • If you activated **password encryption** by using the tag [_to_encrypt_] (see: Encryption of secure information) the included JRE in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/jre** have to support strong AES-256 cryptographic algorithm. This can be easily done and is described here: Usage of AES-256 cryptographic algorithm. Otherwise a RunTimeException occurs which contains: '*Key length (256 bit) is greater than the max allowed key length (128 bit)*'.
The URL in the browser results in a 404 error message.	• Use the Tomcat manager (http://localhost:9090/manager/html) to check if the Product 360 - Supplier Portal application is running. The Tomcat user for log in at the management UI can be configured in **<PIM_SUPPLIER_PORTAL_INSTALLATION_ROOT>/tomcat/conf/tomcat_users.xml**

Problem	Possible solution
There's a spring error in the logs saying that table XYZ is missing.	• Open the Product 360 - Supplier Portal log file to check if the database setup succeeded and all migrations have been applied. Errors related to "flyway" usually point to a failed database setup. • Ensure that the database user has the necessary permissions.
I changed a configuration property but it doesn't work.	• Product 360 - Supplier Portal logs all properties during bootstrap. Change the logging level to INFO to see all found properties and their values.
`SocketException` occurs on Product 360 - Supplier Portal server if many Product 360 - Supplier Portal clients are active.	Increase the number of sockets in the windows registry using RegEdit.exe: Add key: **MaxUserPort** with the value 65534 in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** see also in: • http://www.codeweblog.com/no-buffer-space-available • http://rwatsh.blogspot.de/2012/04/resolution-for-no-buffer-space.html

Tasks cannot be created/assigned to suppliers, i.e. the "Supplier" option is available as assignee in the task creation dialog.	Make sure that the following settongs in the hsx.properties of the Product 360 server are set as follows:
	`hsx.enabled = true`
	`hsx.suppliertasks.enabled = true`

Tasks for suppliers (Task node "Tasks assigned to suppliers") are neither displayed in Desktop nor Web client.	Make sure that the access right "Show tasks for all suppliers" is granted to the respective user group/ organization.

13 Business Process Management

To install the integration of Informatica BPM it is required to perform the following steps in the predefined order:

- Informatica BPM Installation (see page 199)
- BPM specific configuration within server.properties (see page 212)

- Failsafe handling of calls to Informatica BPM (see page 220)
- Message Queue Based Communication (see page 222)
- Delayed message delivery (see page 222)

13.1 Informatica BPM Installation

- Informatica BPM Installation (see page 199)
  - Installation of the Informatica BPM service (see page 199)
  - Webserver and Java (see page 200)
    - Adjusting the webserver to support non SSL port (see page 200)
  - Integrated Security (see page 201)
    - Configuration during installation (see page 201)
    - Re-configuration of already installed server (see page 202)
- Installation of the required default workflows (see page 202)
- Configure Dispatch Services (see page 205)
- Preparing Informatica BPM service for JMS based communication (see page 208)
  - Download additional library (see page 208)
    - ActiveMQ client library (see page 208)
  - Setup messaging service within Informatica BPM (see page 208)
    - Detail configuration of the message manager (see page 209)
      - JMS Messaging Configuration (see page 209)
      - Initial Context Properties (see page 210)
      - Queues & Listeners (see page 211)
    - Verifying the configuration (see page 212)

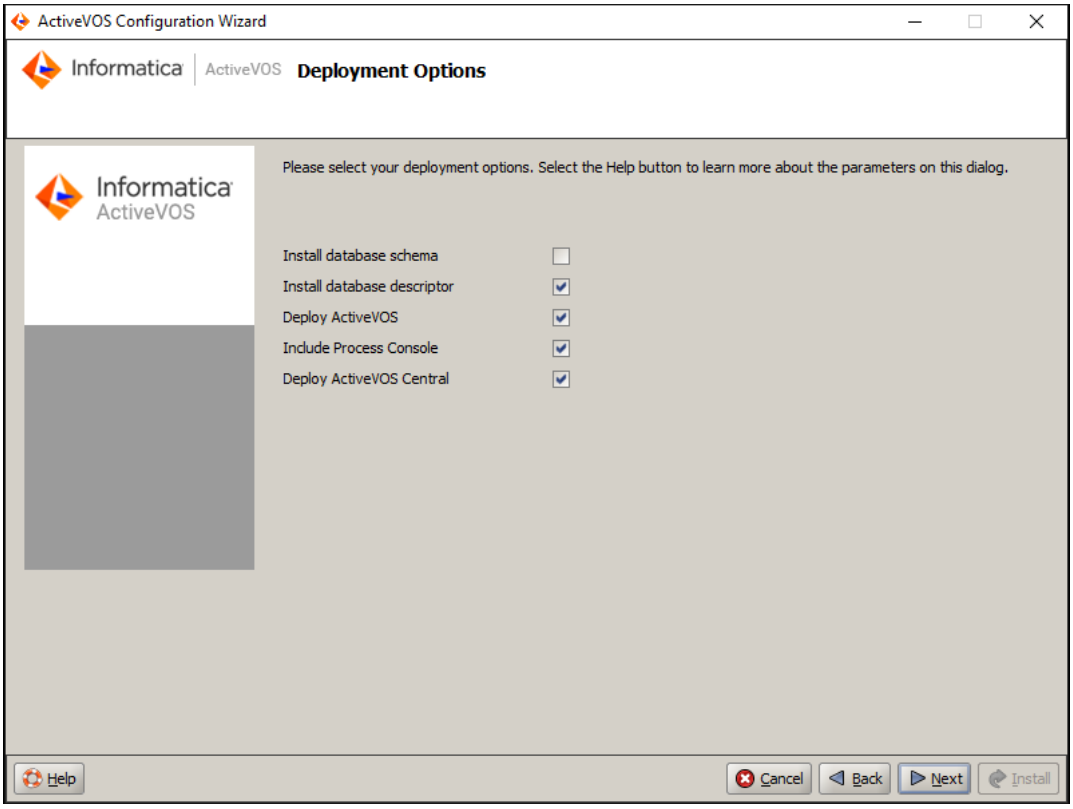
13.1.1 Informatica BPM Installation

13.1.1.1 Installation of the Informatica BPM service

For the installation of the *Informatica BPM service* it is recommended to follow the official installation guide at https://docs.informatica.com/process-automation/informatica-activevos/current-version.html.

In the *Prerequisites* chapter https://docs.informatica.com/process-automation/informatica-activevos/current-version/4-----server-installation--configuration--and-deployment/apache-tomcat/general-information/prerequisites.html you can find the information about database servers supported for ActiveVOS and additional information about database drivers which are supported. The drivers themselves are not included in the installation package of ActiveVOS and should be get from database vendor.

In the past there were some issues occurred during installation of ActiveVOS if the database schemas have been already created before installation.
So please remember to uncheck "*Install database schema*" if empty DB is already created and to check the "*Install database schema*" option if database schema should be created during installation of ActiveVOS.



13.1.1.2 Webserver and Java

A good start is to use the integration with Apache Tomcat as container where *Informatica BPM service* will be deployed to.

We recommend to use a container version equal or newer to Apache Tomcat 8.5.51.

> Make sure to use Java 8 as runtime for the *Informatica BPM service* by setting the necessary environment variables for example.

Adjusting the webserver to support non SSL port

The Informatica BPM web endpoint does enforce SSL by default. To disable that behavior it is possible to set a JVM property:

```
-Dae.web.filter.https.force=false
```

13.1.1.3 Integrated Security

It's possible to configure the "Informatica BPM" Server to use integrated Security for MS SQL Server connection. In this case the configuration files do not contain sensitive security data like database user and password of the database user.

The configuration can be made during the installation and initial configuration of "Informatica BPM" Server and as a post-configuration for already existing installations.

Configuration during installation

In this case it's better to use the silent installation and configuration mode

1. Create a Windows service user which will be used to execute BPM Server. (e.g. INFA\bpm-service)
2. Create the same user as MSSQL Server user and configure this user to use Windows Authentication (INFA\bpm-service)
3. Create manually a new ActiveVOS database and configure the owner of this database to newly created user (INFA\bpm-service).
4. Install the Webserver (in our case it's Apache Tomcat) and copy the SQL Server driver class and the additional dll (*sqljdbc42.jar* and *sqljdbc_auth.dll*) in the *lib* folder of Tomcat
5. Adapt the *service.bat* to use tomcat lib folder additional to a java.lib.path like this: **--JvmOptions** "...; ...;**-Djava.library.path=%CATALINA_HOME%\lib**"
6. Extract the installation and configuration tool for "Informatica BPM".
   Go to the *<installation_tool>\server-enterprise\tomcat_config\bin* folder and adapt the *install.properties* for server configuration. See example for properties relevant to integrated security. The content of username and password is mandatory but not relevant for the connection. So you can use any signs.

   Properties

   ```
   jdbc.database.driver.class=com.microsoft.sqlserver.jdbc.SQLServerDriver
   jdbc.database.driver.jar=<tomcat_path>\\lib\\sqljdbc42.jar
   jdbc.database.url=jdbc\:sqlserver\://
   <sqlserver_host>;databaseName\=Active_VOS;integratedSecurity=true;
   jdbc.database.name=Active_VOS
   jdbc.database.password=xxxx
   jdbc.database.username=xxxx
   ```

7. Go to the *<installation_tool>\server-enterprise\tomcat_config\bin* folder and adapt the *config_deploy.bat* to use tomcat lib folder additional to a java.lib.path like this:

   Configuration

   ```
   "<jdk_path>\bin\java" -Xms128m -Xmx512m -Djava.library.path="<tomcat_path>\lib"
    -jar config.jar %1
   ```

8. Open the command window and execute the *config_deploy.bat* in **silent** mode.
9. Install the Tomcat service using *service.bat install*

10. Configure the "Log on" for this service to use the BPM service account (INFA\bpm-service)
11. Start the service and call the ActiveVOS Console.

Re-configuration of already installed server

Following steps can be made to re-configure the existing BPM Server installation to use the integrated security for database connection:

1. Stop and uninstall the Tomcat service for BPM Server. Use *service.bat uninstall [tomcat service name]*
2. Create a Windows service user which will be used to execute BPM Server. (e.g. INFA\bpm-service)
3. Create the same user as MSSQL Server user and configure this user to use Windows Authentication (INFA\bpm-service)
4. Configure the owner of the existing ActiveVOS database to newly created user (INFA\bpm-service).
5. Go to the webserver (Tomcat) installation ({install_dir}/apache-tomcat/conf/Catalina) and to the BPM server ({install_dir}/server-enterprise/tomcat_config/conf) and adapt activevos.xml and active-bpel.xml in both places to use integrated security (s. example). The content of username and password is mandatory but not relevant for the connection. So you can use any signs like in example.

   Configuration

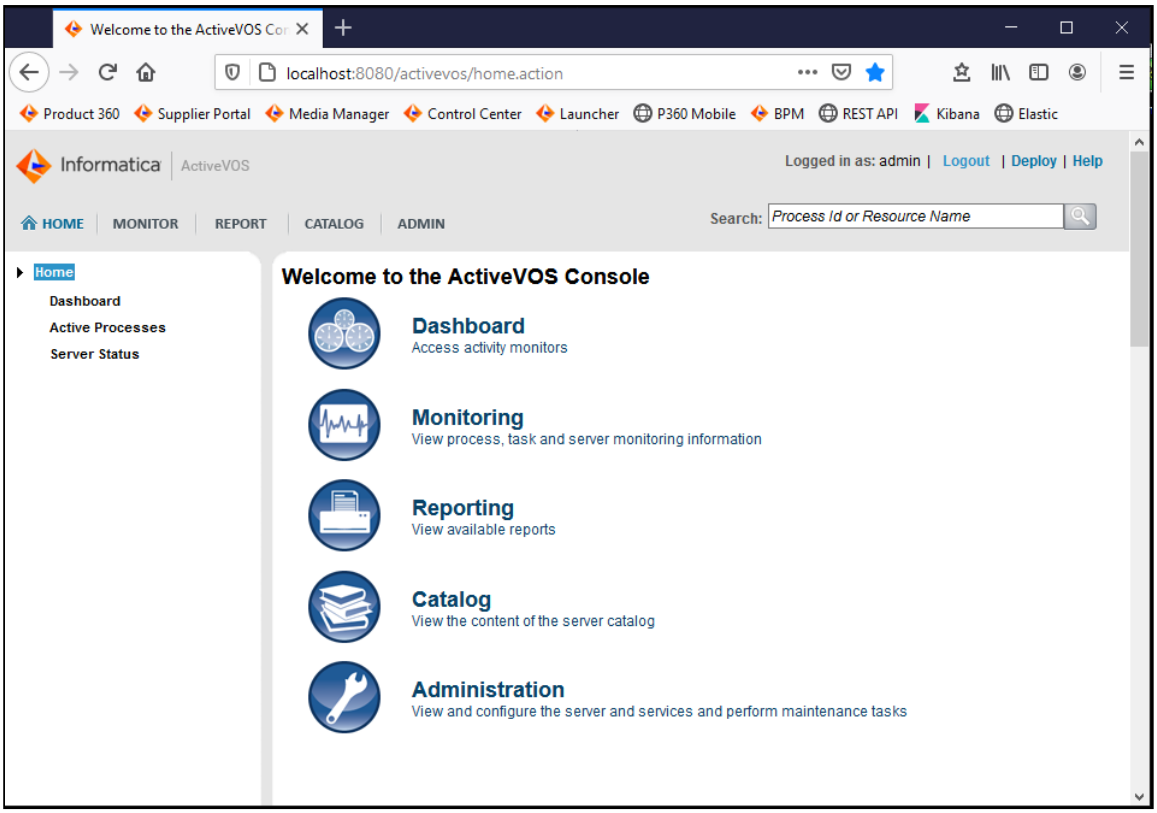
   ```
   <Context displayName="ActiveBPEL Enterprise Tomcat Database context" path="/
   active-bpel">
    <Resource name="jdbc/ActiveVOS" auth="Container" type="javax.sql.DataSource"
        maxActive="100"
        maxIdle="10"
        maxWait="1000"
        username="xxxx"
        password="xxxx"
        driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver"
        url="jdbc:sqlserver://
   server.informatica.com;databaseName=Active_VOS;integratedSecurity=true;"/>
    </Context>
   ```
6. Copy the driver class and the additional dll (*sqljdbc42.jar* and *sqljdbc_auth.dll*) in the lib folder of Tomcat
7. Adapt the *service.bat* to use tomcat lib folder additional to a java.lib.path like this: **--JvmOptions** "...; ...;**-Djava.library.path=%CATALINA_HOME%\lib**"
8. Install the Tomcat service using *service.bat install*
9. Configure the "Log on" for this service to use the BPM service account (INFA\bpm-service)
10. Start the service and call the ActiveVOS Console.

13.1.2 Installation of the required default workflows

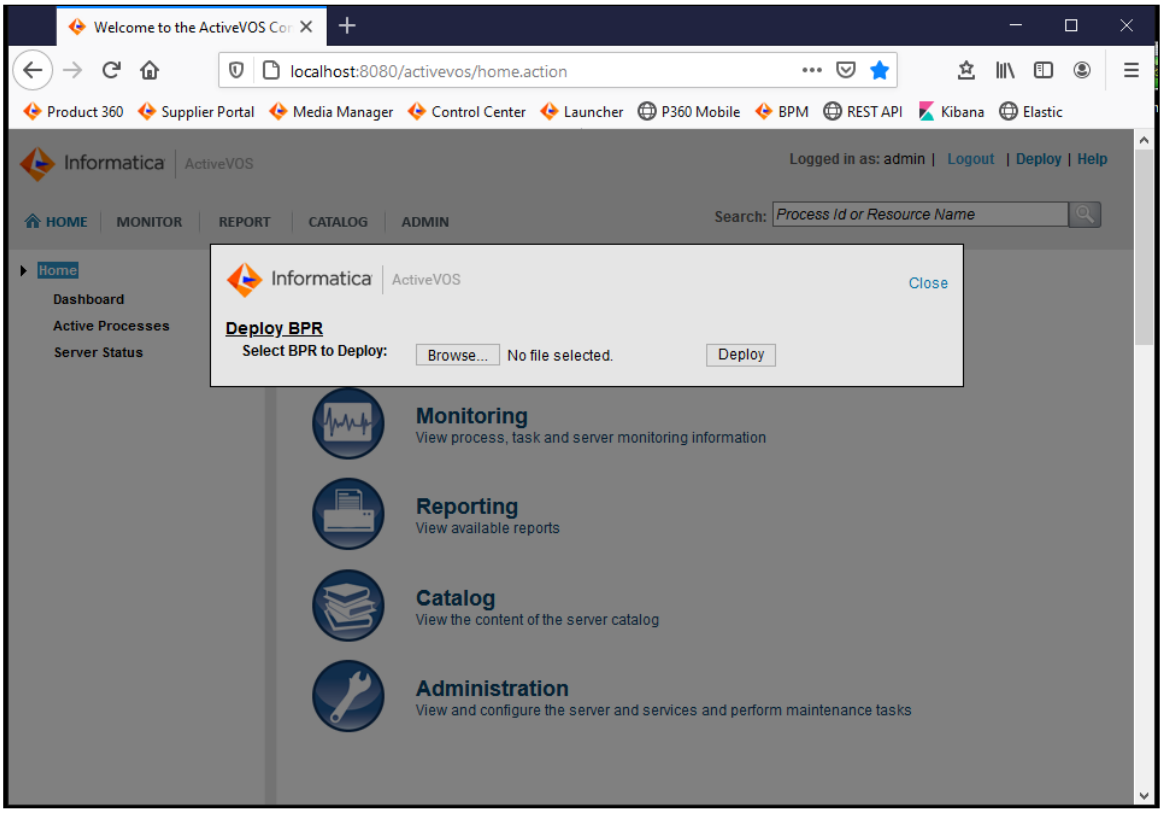
After installing the *Informatica BPM service* the required default workflows have to be deployed to the BPM instance.

The workflows are provided as deployable Business Process Archives: ***P360_JMS_Core.bpr*** and ***P360_BPM_Management.bpr*** in the Accelerator package *<P360 version>_InformaticaBPM* of the P360 release.

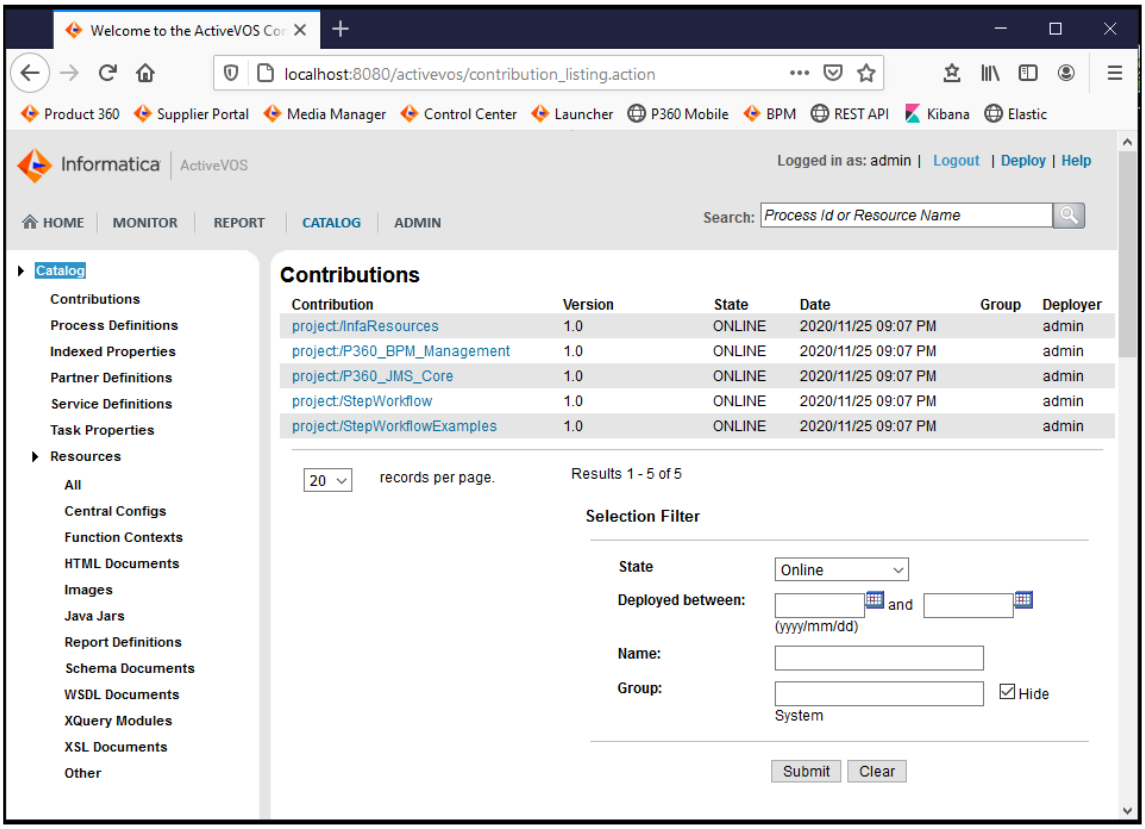
To deploy the workflows make sure the *Informatica BPM service* is up and running: Open your web browser and open the management console located at http://your-bpm-server:8080/activevos. You should see the start page of the management console.



To deploy the workflows open the deploy dialog by clicking on the "Deploy" button in the upper right corner and upload the Business Process Archives.



After the upload and deployment has been processed successfully you can check the availability of the P360 default workflows by navigating to *Catalog/Contributions* where you should now see the deployed projects containing the P360 default workflows in the list.

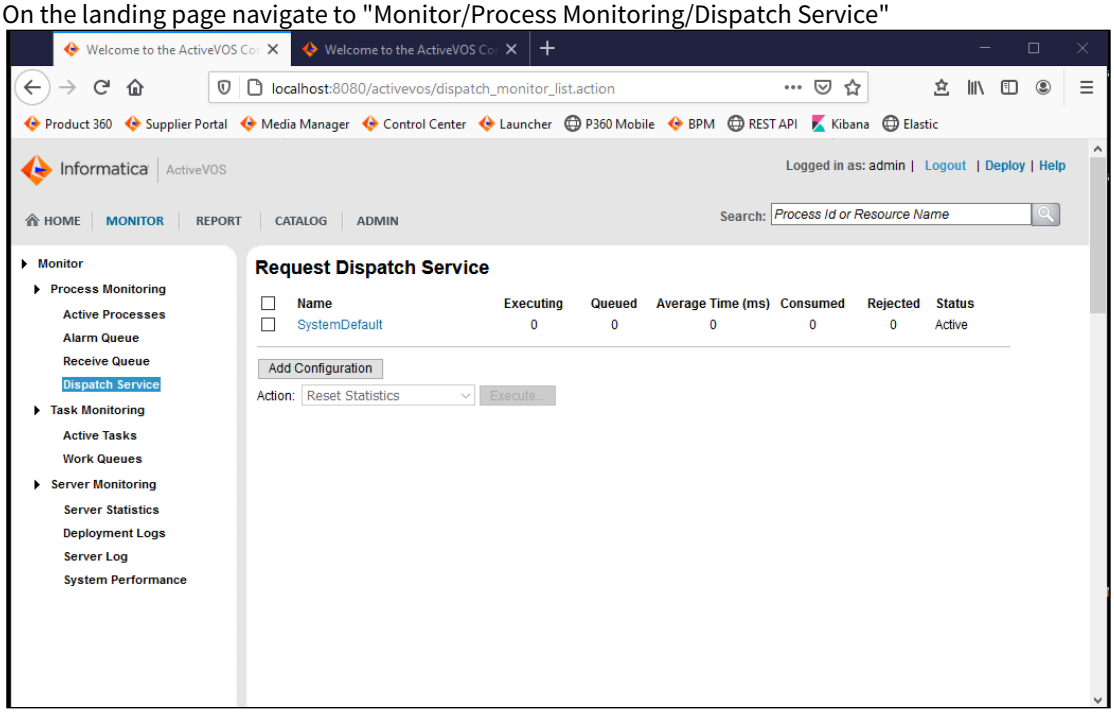


13.1.3 Configure Dispatch Services

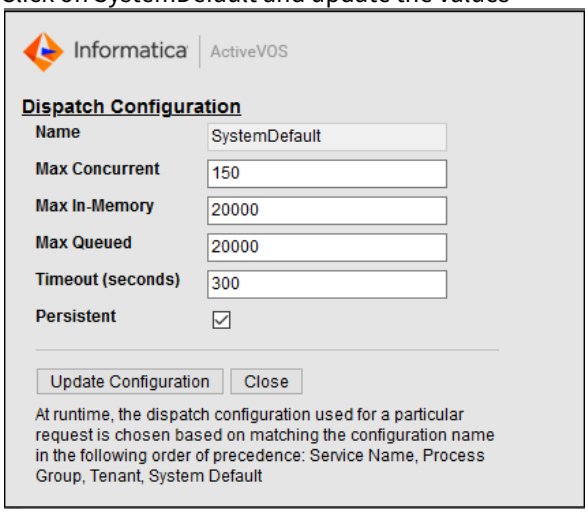
The dispatch services have to be configured in the console of BPM:

1. Open a web browser and navigate to http://your-bpm-server:8080/activevos and login using your user credentials

2. On the landing page navigate to "Monitor/Process Monitoring/Dispatch Service"



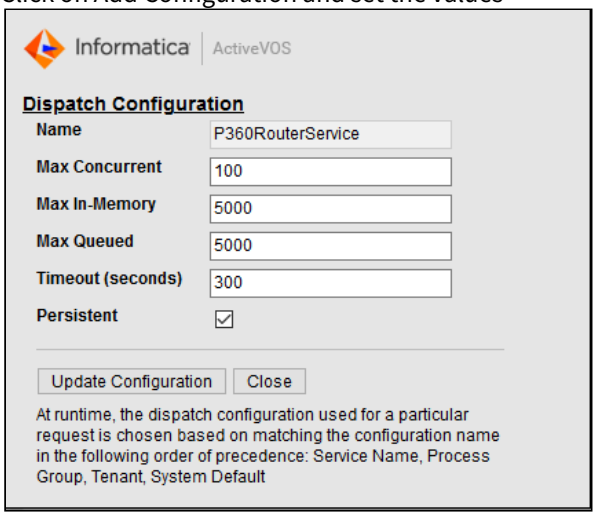
3. Click on SystemDefault and update the values



Dispatch Configuration	
Name	SystemDefault
Max Concurrent	150
Max in Memory	20000

Dispatch Configuration	
Max Queued	20000
Timeout (seconds)	300
Persistent	true

4. Click on Update Configuration
5. Click on Add Configuration and set the values



Dispatch Configuration	
Name	P360RouterService
Max Concurrent	100
Max in Memory	5000
Max Queued	5000
Timeout (seconds)	300

Dispatch Configuration	
Persistent	true

6. Click on Update Configuration

13.1.4 Preparing Informatica BPM service for JMS based communication

The communication between Informatica Product 360 and Informatica BPM service can be switched to an asynchronous message based communication. To enable this capability of Informatica BPM service some post installation steps have to be performed.

13.1.4.1 Download additional library

ActiveMQ client library

To make Informatica BPM service ready for working with messaging an additional library has to be installed.

- Download https://repo1.maven.org/maven2/org/apache/activemq/activemq-all/5.15.9/activemq-all-5.15.9.jar
- Put the downloaded file activemq-all-5.15.9.jar into the *lib* folder of the Tomcat container
- Ensure the JDK version is >=1.8 as the active mq lib requires that

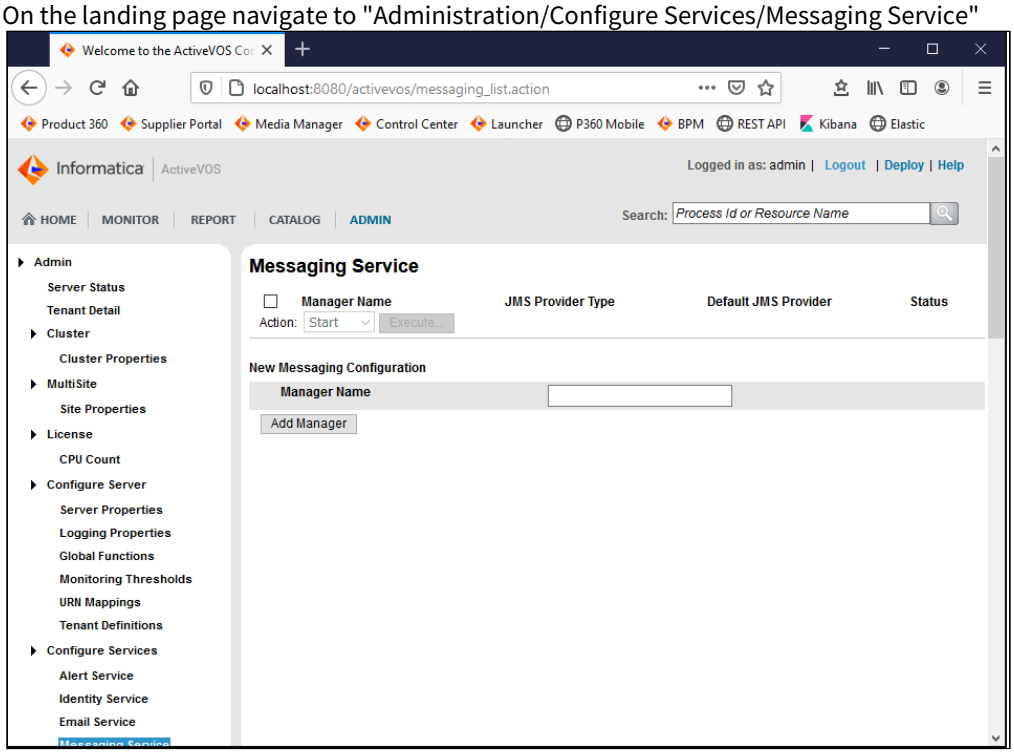
Make sure to restart the Informatica BPM service so that the changes take effect.

13.1.4.2 Setup messaging service within Informatica BPM

To be able to use the asynchronous message based communication between Informatica Product 360 and Informatica BPM service some basic configuration within Informatica BPM has to be set up. This configuration will be done using the Informatica BPM management console.

1. Open a web browser and navigate to http://your-bpm-server:8080/activevos and login using your user credentials

2. On the landing page navigate to "Administration/Configure Services/Messaging Service"



3. Create a new "Manager" entering "ActiveMQ" as name and clicking on the "Add Manager" button
4. A new entry with name "ActiveMQ" will appear in the list of manager, to configure the manager in detail click on the manager entry

Detail configuration of the message manager

To finish the configuration of the manager you have to add the following values as minimum configuration

JMS Messaging Configuration

Property name	**Property value**
Default JMS Provider	enabled
JMS Provider Type	Other JMS
Connection Factory Name	ConnectionFactory
Connection User	The username to connect to the ActiveMQ message broker

Property name	Property value
Connection Password	The password to connect to the ActiveMQ message broker
Send Empty Credentials	disabled
Maximum Total Connections	-1
Maximum Free Connections	15
Delivery Mode	Persistent
Time To Live (ms)	0
Priority (int)	0
Reconnect Interval (ms)	

Initial Context Properties

Property name	Property value
java.naming.provider.url	tcp://your-activemq-server:61616?jms.redeliveryPolicy.maximumRedeliveries=-1 [1]
java.naming.factory.initial	org.apache.activemq.jndi.ActiveMQInitialContextFactory
queue.JNDI_P360_BPM	P360_BPM
queue.JNDI_P360_SERVICE_API	P360_SERVICE_API

Property name	Property value
queue.JNDI_P360_BATCH_API	P360_BATCHAPI
queue.JNDI_P360_BPM_RESPONSE	P360_BPM_RESPONSE

[1] if using ssl connection make sure to import the corresponding certificates into jour JREs trust store.

Queues & Listeners

Add a new entry in section Queues & Listeners, not mentioned properties need to stay with their default value

Property name	Property value
Name	P360_BPM_LISTENER
JNDI Location	JNDI_P360_BPM
Listener Class	com.activee.rt.mom.jms.transport.AeJmsBpelListener
Listener Count	15
Default Service	P360RouterService

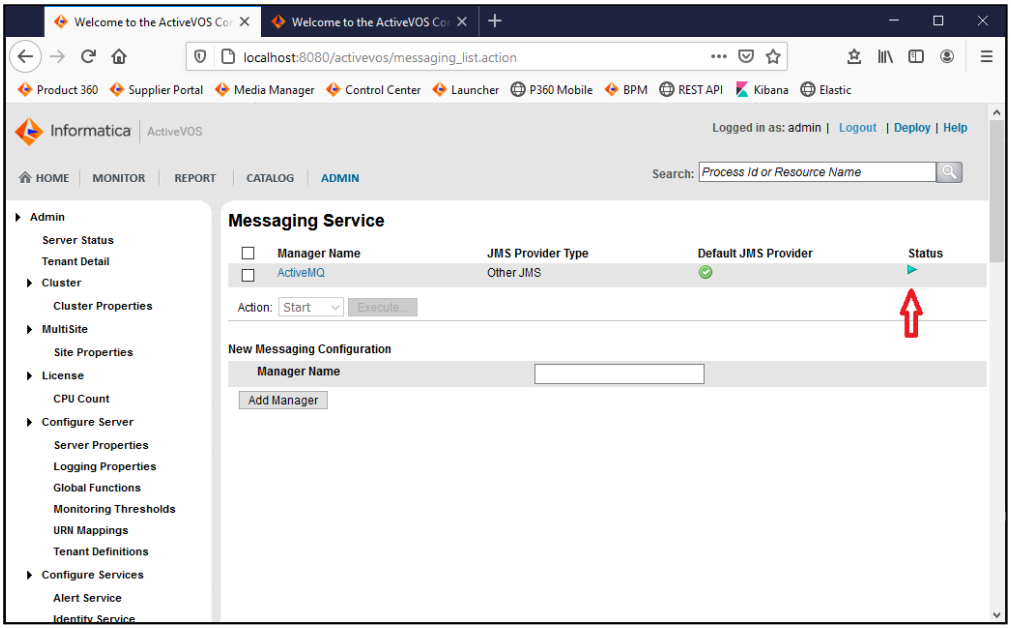
Add a new entry in section Queues & Listeners, not mentioned properties need to stay with their default value

Property name	Property value
Name	P360_BPM_RESPONSE_LISTENER
JNDI Location	JNDI_P360_BPM_RESPONSE

Property name	Property value
Listener Class	com.activee.rt.mom.jms.transport.AeJmsBpelListener
Listener Count	15
Default Service	P360RouterService

Verifying the configuration

After the manager configuration has been validated and saved you can go back to the Messaging Service overview page. Your manager should now appear in the list with status running.



13.2 BPM specific configuration within server.properties

Once the "Informatica BPM" instance is up and running it's time to do the necessary configuration on Product 360 side. The configuration has to be done in the **<P360_SERVER_INSTALLATION_ROOT>\configuration\HPM\server.properties** file of the Product 360 server application.

The integration supports two communication strategies: REST and message queue. The direct REST communication is deprecated and will be removed in future versions. The message queue communication mode should be used for new installations.

The configuration properties of both strategies are different and documented in the following sections.

13.2.1 Message queue communication properties

Property name	Required	Default value	Description
infa.bpm.trigger.queue.ids	Yes	bpm	Comma separated list of queue ids, which are available in the trigger configuration. The first entry of this list represents the default response queue, which is used e.g. if a message from BPM does not specify any response queue id.
infa.bpm.consumer.serviceapi.queue.ids	Yes	serviceapi	Comma separated list of queue ids, for which a service API consumer is applied. This allows to define multiple service API consumer instances with different thread count and message selectors on the same physical queue.
com.heiler.ppm.bpm.server/proxy	No		Allows to track service API consumer requests using a proxy like Fiddler web debugger, example is localhost:8888 This property is disabled by default.

Message queue settings:

Property name	Required	Default value	Note
queue.bpm.type	Yes	${queue.default.type}	
queue.bpm.writer.count	Yes	${queue.default.writer.count}	Number of threads which puts events on the physical message queue
queue.bpm.consumer.count	Yes	${queue.default.consumer.count}	

Property name	Required	Default value	Note
queue.bpm.url	Yes	${queue.default.url}	
queue.bpm.username	Yes	${queue.default.username}	
queue.bpm.password	Yes	${queue.default.password}	
queue.bpm.message.format	Yes	XML	XML is the only message format possible at the moment
queue.bpm.name	Yes	P360_BPM	Physical queue name with the system.name property as prefix
queue.bpm.label	Yes	BPM	Label shown in the trigger configuration view
queue.serviceapi.type	Yes	${queue.default.type}	
queue.serviceapi.writer.count	Yes	${queue.default.writer.count}	
queue.serviceapi.consumer.count	Yes	${queue.default.consumer.count}	Number of queue consumer threads which process events from the message queue
queue.serviceapi.url	Yes	${queue.default.url}	
queue.serviceapi.username	Yes	${queue.default.username}	

Property name	Required	Default value	Note
queue.serviceapi.password	Yes	${queue.default.password}	
queue.serviceapi.message.format	Yes	XML	Can be JSON/XML
queue.serviceapi.name	Yes	P360_SERVICE_API	Physical queue name with the system.name property as prefix
queue.serviceapi.label	Yes	Service API	

It is possible to define own queue configurations with custom queue ids. The syntax is queue.[queue id].*

To disable the prefix of physical queue names by the system.name property add following setting:

com.heiler.ppm.messagequeue.server/useSystemNamePrefix = false

13.2.2 General properties

Property name	Required	Default value	Description
infa.bpm.taskRefreshInterval	No	10	Time interval in seconds in which task update events are executed. This relates to task update events which are triggered by a call to workflow status updates.

13.2.3 REST communication properties

Property name	Required	Default value	Description
infa.bpm.base.url	Yes	http://localhost:8080/active-bpel	The base url to the Informatica BPM instance in the form http://[server]:[port]/active-bpel
infa.bpm.workflows.path	Yes	services/REST	The workflows path. Will be used together with the property **infa.bpm.base.url** to find the endpoints
infa.bpm.user	No		The username for accessing the Informatica BPM instance. Only required if basic authentication on BPM side is configured
infa.bpm.password	No		The password for accessing the Informatica BPM instance. Only required if basic authentication on BPM side is configured If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
com.heiler.ppm.bpm.server/proxy	No		Allows to track any call from the server to the Informatica BPM system using a proxy like Fiddler web debugger, example is localhost:8888 This property is disabled by default

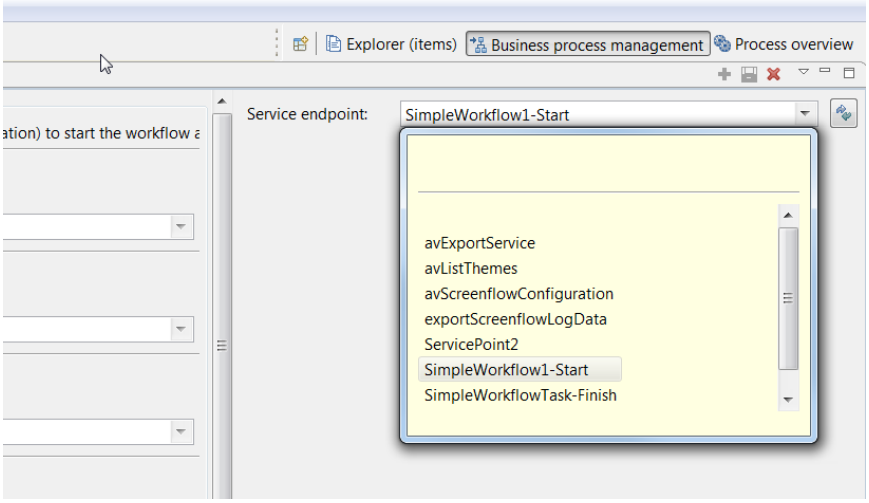
Property name	Required	Default value	Description
infa.bpm.serviceendpoint.filter	No		Comma separated list, possibility of filtering out specific service endpoints, e.g.:serviceEndpoint1, serviceEndpoint2
infa.bpm.maxRequestRate	No	unlimited	Maximum rate of requests per second which are run against the BPM backend.
infa.bpm.taskRefreshInterval	No	10	Time interval in seconds in which task update events are executed. This relates to task update events which are triggered by a call to workflow status updates.
infa.bpm.serviceEndpointListPollInterval	No	5	Time interval in seconds in which the list of endpoints is retrieved from BPM.
infa.bpm.queue.jms.connection.url	No	uses the Audittrail configured JMS connection url	Connection url to the JMS queue. By default this is the same as for Audittrail.
infa.bpm.queue.threadpool.size	No	Number of processor cores	Number of threads which are consuming the internal queue and do call BPM with messages.
infa.bpm.queue.inMemoryBackupSize	No	10000	The number of in memory queued messages, which are stored if no JMS queue is available.
infa.bpm.queue.throttlingDelayMiliseconds	No	10000	The delay in milliseconds which the dispatch of messages is hold before the next try, if BPM is not available anymore.

Property name	Required	Default value	Description
infa.bpm.queue.messageLifetimeHours	No	96	The duration of messages that are queued in hours. If the duration is exceeding the defined time the messages will be deleted.
infa.bpm.logAccumulationDurationInSeconds	No	3600	The time period in which the same exceptions regarding the connection and bpm messages are accumulated before being logged out again

Some of the properties are also responsible for the fail-over handling, for details of these configuration properties please refer to Failsafe handling of calls to Informatica BPM (see page 220) .

13.2.3.1 Simple connectivity test

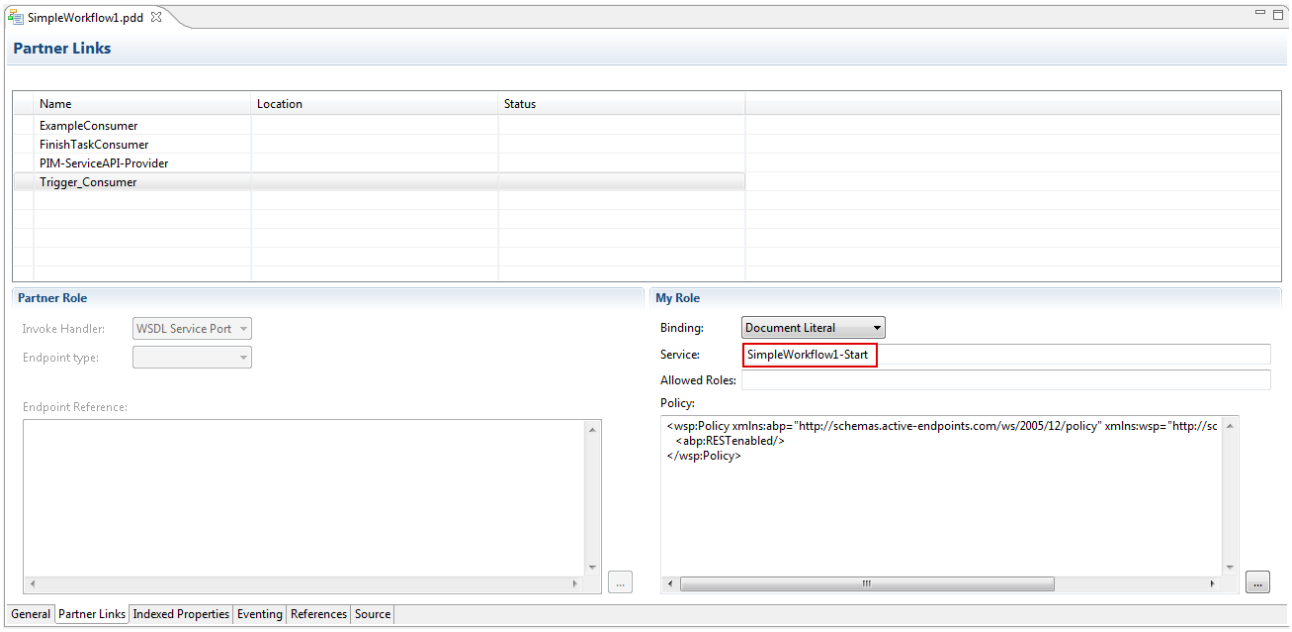
After installing the Informatica BPM service and configuration of the required properties on Product 360 side a first connectivity test can be done by opening the rich client with the "Business process management" perspective. In this perspective a new workflow trigger can be defined and available service endpoints can be assigned.



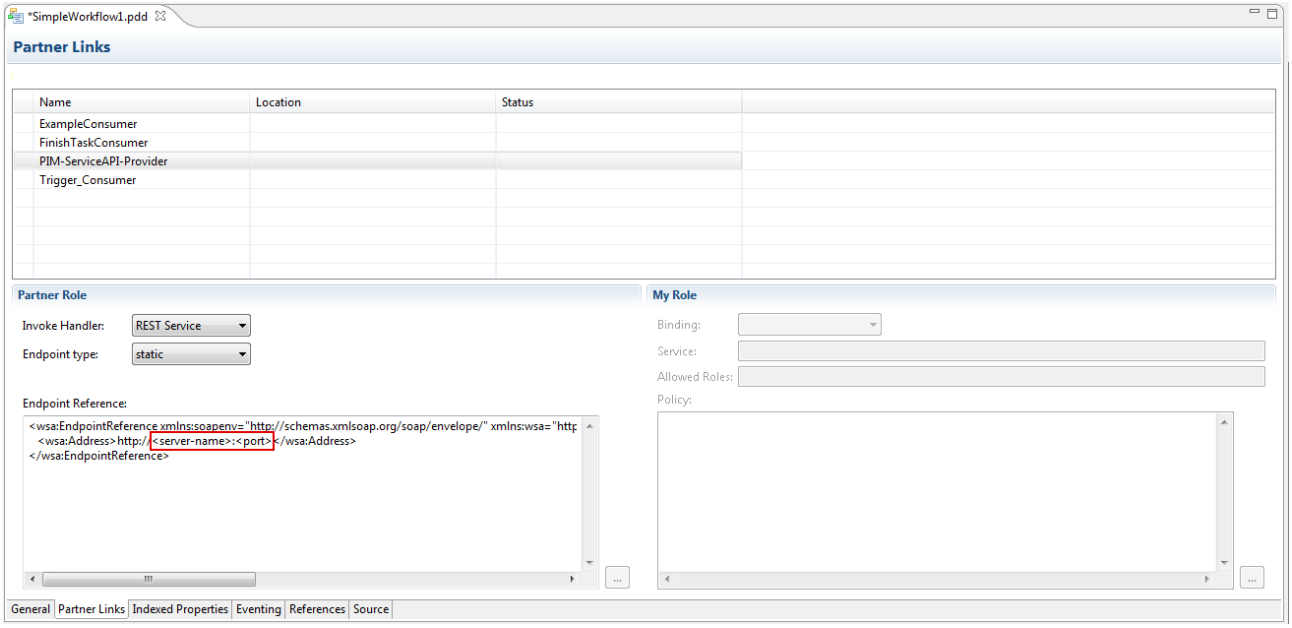
The drop-down list "Service endpoints" contains all service endpoints deployed to the Informatica BPM instance.

13.2.3.2 Service endpoints and partner links within Informatica BPM workflows

Service endpoints of Informatica BPM workflows have to be defined in form of so called partner links in the PDD file of the respective workflow.



The communication between Informatica BPM and Product 360 is performed via Product 360's REST service. The Product 360 server over which the communication should take place has to be made available also by means of a partner link in the workflow's PDD file.



13.3 Failsafe handling of calls to Informatica BPM

Info

This way of fail safe handling is deprecated since 10.0 as the communication between Product 360 server and the BPM engine does now support a message queue mode. See Message Queue API (see page 222) page.

To provide failsafe capabilities for calls to the Informatica BPM engine, there are two strategies available:

- messages are buffered within a JMS message queue (See JMS in Product 360)
- messages are buffered in memory

The JMS message queue solution offers the possibility to buffer a high number of messages and persist them, but fails if the network connection is broken also. This can be declared as high resilient solution against system failures.

The in memory queue solution has limited capacity and the data is lost if the Product 360 server is shut down.

It is possible to configure one, both or no solution at the same time. In the case both (JMS queue and in-memory queue) are configured, the JMS queue is used as a first failsafe queue and in-memory queue as a backup queue if the JMS connection not available.

The configuration has to be done in the **<P360_SERVER_INSTALLATION_ROOT>\configuration\HPM\server.properties** file of the P360 server application.

The following properties are relevant for the failsafe handling of calls to Informatica BPM:

Property name	Default value	Example	Required	Description
infa.bpm.queue.jms.connection.url	uses the audittrail configured jms connection url	tcp://localhost:61616	if JMS queue should be enabled	connection url to the JMS message queue broker. If left empty the JMS queue will be disabled
infa.bpm.queue.inMemoryBackupSize	10000		If in memory queue should be available this has to be >0	the capacity of the in memory queue. If set to 0 the in memory queue will be disabled

Property name	Default value	Example	Required	Description
infa.bpm.queue.threadpool.size	50		no	Number of parallel working threads to process queued messages
infa.bpm.queue.throttlingDelayMiliseconds	10000		no	Forced retry delay if a call to Informatica BPM has failed before
infa.bpm.queue.messageLifetimeHours	96		no	If messages are queued they will expire after the given amount of hours
infa.bpm.queue.jms.connection.username			no	Username if authentication is required
infa.bpm.queue.jms.connection.password			no	Password if authentication is required If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.

Property name	Default value	Example	Required	Description
infa.bpm.queue.jms.queue.suffix			no	A suffix that will be appended to the default queue name ("infa.bpm"). The suffix can contain characters a-z, 0-9

13.4 Message Queue Based Communication

Please see the Integration section of the Customizing Manual for details on how to use the new Message Queue API.

13.5 Delayed message delivery

13.5.1 Objective

This document describes the delivery delay handling in the communication over the message queue in a multi server context.

> **Updates in recent Hotfixes!**
>
> With the current hotfixes of Version 10.0 and 10.1 we were able to introduce a priority server cache invalidation which typically is executed in way under 50 milliseconds.
> In earlier releases the synchronization delay could be multiple seconds. Still, there is a synchronization gap between the servers, even if it's very small now. So we still recommend to configure the Active MQ cluster like describen on this page. The default setting for the delay has been adjusted to 50 milliseconds which makes this delay now unnoticeable to the user.

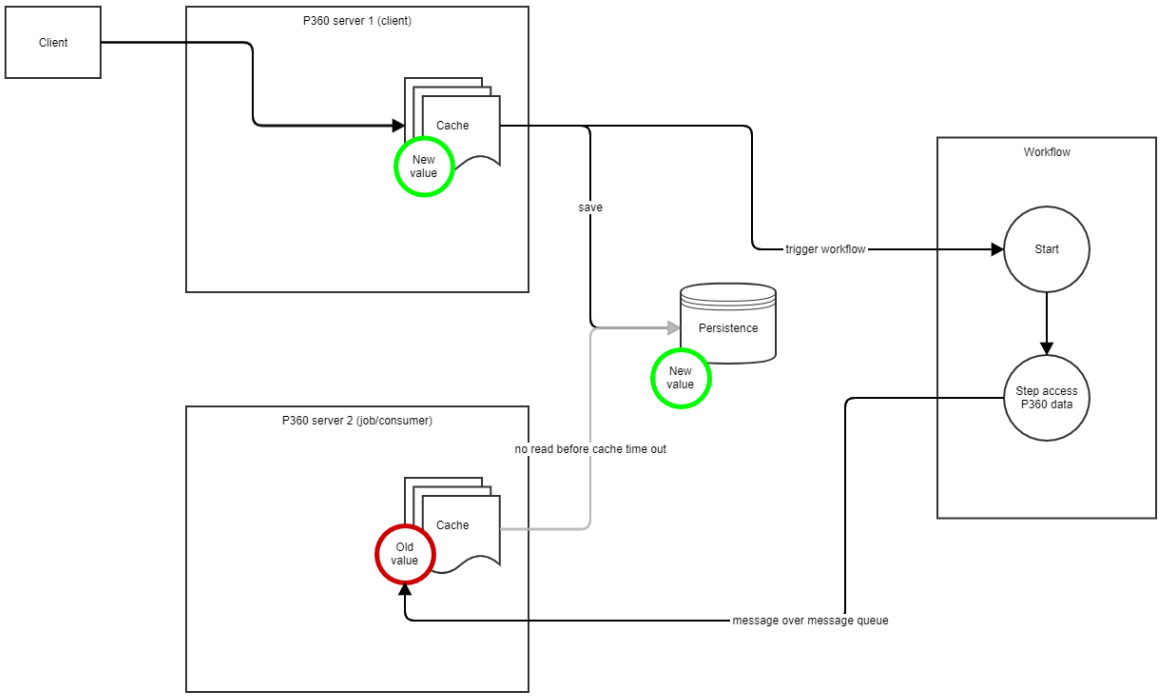
13.5.2 General

The multi-server deployment of Product 360 is designed in a way to allow the highest form of independence of the servers in order to minimize any overhead which would be introduced through excessive locking mechanisms. Each server makes sure that concurrent data modification of the same object is synchronized. It's the nature of a highly scale able architecture like this that caches might be outdated for a short time as change events are delivered asynchronously. The application logic anticipates this delay and compensates by only persisting what is really modified - thus we do not update the database with old data and simultaneously keep the synchronization times to an absolute minimum.

If in that environment the client is connected to **server 1** and the **client does make a change to the persisted data values**, and that change triggers a workflow instance that is communicating over the message queue

with server 2, it might be that **server 2 cannot see the persistence value changes** done by server 1 in the case that the workflow execution and message transport is faster than the cache invalidation event.

To avoid that a workflow can run into this problem, there is a **delivery delay** introduced for outgoing queue messages to the workflow. The delivery delay ensures the Informatica BPM server will get the message only after the delivery delay has passed and not earlier. The default setting for the delivery delay is **50 milliseconds** in a multi server environment. The delivery delay is handled by the message queue instance itself, which introduces the need, that the **message queue server is configured to provide that functionality**.



It's important to note that workflows will be **triggered** with a minimum **delay of 50 milliseconds** with these settings.

13.5.3 Configuration

13.5.3.1 Configuration of Active MQ server

To enable the message delivery delay feature the `activemq.xml` file in the conf folder of the Active MQ server has to be adjusted in the way that the scheduler support is activated:

```
<broker [...] schedulerSupport="true">
...
</broker>
```

After the adjustment the Active MQ instance has to be **restarted**.

13.5.3.2 Product 360 configuration (server.properties)

It is possible to configure the delivery delay on a per queue basis. As a **default** a **50 milliseconds** interval is used in the multi server environment (in a single server env it is 0 milliseconds).

To configure a single queue to have a different deliver delay [milliseconds] use the following syntax:

```
queue.[queue id].delivery.delay = 50
```

Per default this value is written into the Active MQ specific message header called `AMQ_SCHEDULED_DELAY`, but it is possible to overwrite this header key with the following syntax:

```
queue.[queue id].delivery.delay.header = AMQ_SCHEDULED_DELAY
```

Note: the value is always written as a numerical long as header type.

14 Web Search Installation

Please follow the predefined order of the following subsections to prepare the individual Informatica Product 360 modules for use with the Informatica Product 360 - Web Search.

- Pre-Installation Checklist (see page 224)
- Web Search Integration (see page 226)
- Installation Troubleshooting (see page 230)

> **Tip**
>
> If you have any question, how to configure Web Search, have a look to the HowTo page: Web Search Configuration How to
>
> and to the Product 360 - Web Search Configuration page.

14.1 Pre-Installation Checklist

> Product 360 - Web Search is installed as a part of Product 360 - Server Installation. Product 360 - Web Search is powered by Elasticsearch and the Elasticsearch server needs to be installed separately.

> *Elasticsearch is a third party application neither developed nor shipped directly by Informatica. Therefore it is recommended to check install and guideline documentation directly on the website of the vendor to follow best practices.*

14.1.1 Version Requirement

Product 360 - Web Search is compatible with Elasticsearch version 7.x

14.1.2 License Requirement

The Elasticsearch server is available under multiple different licenses.

- Basic (Elastic License) or higher license is recommended

14.1.3 System Requirements

It is recommended that you deploy the Elasticsearch server separately on a single machine or cluster of machines. With the data volume increase, extra nodes should be added in cluster for better performance

14.1.3.1 Memory Requirement

The Elasticsearch server needs lot of memory, that is completely allocated at start time ensuring a fast search index build and a web search.

- 32 GB is recommended
    - In case of indices having multi-PPD hierarchy and large amount of data, then RAM may need to be increased

> Elasticsearch heavily relies on the filesystem cache in order to make search fast. In general, at least half the available memory should go to the filesystem cache.

14.1.3.2 Hardware Requirement

The Elasticsearch server needs fast drives and fast CPU, that is completely allocated at start time ensuring a fast search index build and a web search.

- 512 GB SSD is recommended
- 8 CPU cores is recommended
    - In case of indices having multi-PPD hierarchy and large amount of data, then number of CPU may need to be increased

> It is recommended to always use local storage, remote filesystems should be avoided.

14.1.4 Security Requirement

It is recommended to enable the security pack provided by Elasticsearch, so that Product 360 - Web Search can communicate with Elasticsearch over a secured HTTPS connection.

> **Elasticsearch security**
>
> It is recommended to secure the Elasticsearch cluster in all aspects by following the steps from official documentation at https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-security.html

14.1.5 Further Reading

It is recommended to follow the best practices and settings guidance defined in the Elasticsearch website while setting up the Elasticsearch server.

14.1.6 Elasticsearch Installation on Windows

- Download the zip from any of the locations listed below
  - https://www.elastic.co/downloads/past-releases/elasticsearch-7-11-0
- Extract the zip file
- Go to *bin* folder and open command prompt
  - run the below command
    bin>elasticsearch
- Server will start and is accessible at below url

  http://localhost:9200/_search

14.2 Web Search Integration

14.2.1 Prerequisite

Before you can start with this chapter, you need to have finished the following parts:

- Server Installation (with Control Center)
- Desktop Client Installation (see page 95)

14.2.2 Setup Product 360 Permissions for Web Search

There are 2 different kinds of **Product 360 Core Users** for different Product 360 - Web Search use cases:

1. **Product 360 - Web User**
   - This user runs search queries from within the User Interface of Product 360 Web.
2. **Product 360 - Desktop User**

- This administrator user manages the search indices from within Product 360 Desktop. He can manually create indices, trigger or schedule the incremental index updates.

14.2.2.1 Permission Settings for Product 360 - Web User to use Web Search

The **Product 360 - Web User** need the following **interface visibility rights** at least:

No.	Rights	Type	Category	Permission
1	Interface Visibility	Informatica Product 360 view	Search Index	Search Index

It is recommended to set all necessary Product 360 - Web permission as described in: Product 360 - Web Configuration.

14.2.2.2 Permission Settings for Product 360 - Desktop User to use Web Search Index Build

The **Product 360 - Desktop User** needs the following **action rights**:

No.	Rights group	Permission
1	Export	Export Format Template, general access
2	Export	Export Profile, general access

Please ensure to have all permission to entities, fields and attributes that are defined in the index configuration.

14.2.3 Setup Configuration for Product 360 - Repository

The entities, sub-entities and their fields which are defined for Web Search should be enabled for **export** on Product 360 - Repository in the file **Repository.repository**, located in **<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM**.

The Product 360 Server has to be restarted in order to have changes take effect.

14.2.4 Setup Configuration for Product 360 - Core

The configuration properties for Web Search on Product 360 Core can be defined in the property file **server.properties**, located in **<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM**.

The Product 360 Server has to be restarted in order to have changes take effect.

No.	Property	Default Value	Description	Remarks
1	system.name		Specifies the name of the system	Specifies the name of the system, e.g. Test System / Productive System / Demo / Poad etc. The system name will also be used as a prefix for fulltextsearch index name. Blanks will be replaced with _. Best practice: use 0-9A-Za-z.-
2	fulltextsearch.enabled	true	Enable/disable full-text search	Full-text search can be enabled (default) or disabled. If full-text search is enabled, ensure you setup the Elasticsearch integration properties.

No.	Property	Default Value	Description	Remarks
3	fulltextsearch.rest.url	http://localhost:9200	URL path to the Elasticsearch REST server.	Depending where the Elasticsearch server is located, the server name (e.g. **localhost**) and port (e.g. **9200**) can be different. Incase a multi-server Elasticsearch cluster is created, a comma separated list of the server name and port should be provided. E.g. elasticsearch.rest.url = http://localhost:9200,http://localhost:9201
4	fulltextsearch.rest.user		Login name of the Elasticsearch REST server.	If not using user and password combination, please leave this **field empty, but active**
5	fulltextsearch.rest.password		Login password of the Elasticsearch REST server.	If not using user and password combination, please leave this **field empty, but active**
6	fulltextsearch.rest.allow.self-signed.certificate	true	Allows self-signed certificate only if you use `https`.	

14.2.5 Setup Configuration for Product 360 - Desktop

The search index can only be created, if the **fulltextsearch.enabled=true** in **server.properties.**

In order to create a search index,

1. An **export format template** needs to be defined with -
    - Purpose - **Full-text search**
    - Post-processing export step - **Search index synchronization**
    - File management -
        - Extended options - **true**
        - Output files -
        - **config-file**
            - Format - JSON
            - Encoding - UTF-8
        - **data-file**
            - Format - JSON
            - Encoding - UTF-8
2. An **Full-text search profile** needs to be defined using the above **export format template** and executed.
3. This **Full-text search profile** will create a search index in the Elasticsearch server.
4. The above **Full-text search profile** should be scheduled to run for incremental indexing.

14.2.6 Setup Configuration for Product 360 - Web

The configuration properties for Web Search on Product 360 Web can be defined in the property file **webfrontend.properties**, located in **<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM**.

No.	Property	Default Value	Description
1	`web.client.hps.max.display.facet`	5	Maximum number of displayed search facets.

14.3 Installation Troubleshooting

In case the application doesn't work, you might try the following:

Problem	Possible solution
Building search index failed on Product 360 Desktop in the Process Overview Perspective → Publications → Full-text search	• Literal errors: The index configuration is not error tolerant. You have to use the exact entity, sub-entity and field identifier definition from Product 360. Please have a look to the index example how it should look like. • Time to time the example files will be updated to demonstrate the new supported index settings. • There are no read permission of some entities, sub-entities or fields to the user triggering the indexing. • There are no export purpose of some entities, sub-entities or fields to the user triggering the indexing. • Product 360 Server is running without variants although the search index configuration is based on variants. • The search index configuration defines a catalog which is unknown in Product 360.

Problem	Possible solution

No search results	Please check:
	• Product 360 Server and Elasticsearch Server is available
	• Index build was successful
	  • Check the job summary in Process Overview Perspective → Publications → Full-text search
	• Use for the first time an asterisk '*' as a search string
	• Check all index configuration settings in:
	  • **<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM\webfrontend.properties**
	  • **<PIM_SERVER_INSTALLATION_ROOT>\server\configuration\HPM\server.properties**
	• May be the Product 360 data has not anything which matches the search string

Drill-Down functionality does not work	Please check in the index configuration:
	• Define **more than one** entity in the **rootEntities**
	• Define **parentIdentifier** key in the child root entity
	  • E.g. For **"Article"** define **parentIdentifier = "Product2G",** for a 2PPD system
	  • E.g. For **"Article"** define **parentIdentifier = "Variant"** and for **"Variant"** define **parentIdentifier = "Product2G"** for a 3PPD system
	• In the export modules, define a field **"RecordJoin"** which joins the child record to its parent record.
	• In the export modules, define a field **"routing"** which routes the child record to where its parent record is located.
	  • In a 2PPD system, both **Product2G** record and **Article** record should have the **same routing** key and the routing key is defined by the **Product2G** record.
	  • In a 3PPD system, **Product2G** record, **Variant** record and **Article** record should have the **same routing** key and the routing key is defined by the **Product2G** record.

Object rights will not be considered	Object rights field i.e. "**Acl**" field of Item, Variant and Product2G entities will be automatically added to the index configuration. In the export modules, the "**Acl**" field needs to be populated - • Product2G → "Acl":"{&Product.Object rights.Internal identifier}" • Article → "Acl":"{&Item.Object rights.Internal identifier}" • Variant → "Acl":"{&Variant.Object rights.Internal identifier}"

Copyright

© Copyright Informatica LLC 1993, 2024

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica and the Informatica logo are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade names or trademarks of their respective owners.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.