



Installation

Informatica MDM - Product 360

Version: 8.1.1

1 Table of Contents

1	Table of Contents	2
2	Pre-Installation Checklist.....	12
3	Logical Service Overview.....	12
4	General Communication Overview	13
5	Port Overview	13
5.1	Database	13
5.2	Server, Web and Desktop.....	14
5.3	Media Manager	14
5.4	Port range.....	15
5.4.1	Supplier Portal.....	15
5.4.2	Audit Trail	16
5.4.3	Web Search	16
6	Step by Step installation guide.....	16
6.1	Pre-Requisites	16
6.1.1	Pre-Requisites for Product 360 Supplier Portal	16
6.1.2	Pre-Requisites for Active Vos.....	16
6.1.3	Documentation.....	17
6.1.4	Operating system.....	17
6.1.5	Application and install file matrix	17
6.2	Installation of Product 360 applications	18
6.2.1	1. Installation of the Product 360 Server.....	18
	1.1 Installation of the database	18
	1.2 Installation of the Product 360 Control Center.....	18
	1.3 Installation of the Product 360 Application server.....	18
6.2.2	2. Installation of the Product 360 Desktop Client.....	19
6.2.3	3. Installation of the Product 360 Supplier Portal.....	19
	3.1 Installation of the database	19
	3.2. Installation of Supplier Portal	19

6.2.4	4. Installation of Active Message Queue.....	19
6.2.5	5. Installation of Product 360 Audit Trail	20
	5.1 Installation of the database	20
	5.2 Installation of Audit Trail	20
6.2.6	6. Installation of BPM / ActiveVos	20
	6.1 Installation of the database	20
	6.3 Create a Active Vos root folder.....	20
	6.2 Installation of Tomcat	21
	6.3 Installation of JDK	21
	6.4 Installation of SQL driver	21
	6.5 Installation of Active Vos	21
	6.6 Installation of BPM	21
6.2.7	7. Installation of Websearch	21
	7.2 Installation of Websearch	21
6.2.8	8. Installation of Product 360 Media Manager	22
	8.1 Installation of the database	22
	8.2 Installation of the Media Manager.....	22
7	Database Installation	22
7.1	Pre-Installation Checklist.....	22
7.1.1	Database Administration Tool	22
7.1.2	Database Information	22
7.1.3	Default Product 360 Database Ports.....	22
7.2	DBMS Installation and Configuration Hints	23
7.2.1	Microsoft SQL Server.....	23
	Server Settings	23
	Named-Instance Support	25
7.2.2	Oracle.....	26
	Server Settings	26
	Database User Settings	28
	DBA Tasks	28
7.3	Server Database.....	28
7.3.1	Custom Indexes	28
7.3.2	Oracle RAC, Oracle ASM (Automated Storage Management)	29
7.3.3	Minimum Oracle privileges.....	31
	Normal installation (tablespaces and db users are not existing before install process).....	31

Installation with restricted privileges (similar update)	32
7.3.4 Binaries	33
Creating/Updating schemas - Microsoft SQL Server (GUI)	38
Creating/Updating schemas - Oracle (GUI)	41
Creating/Updating schemas (Headless)	44
7.3.5 Troubleshooting	44
7.4 Media Manager Database	44
7.4.1 Installing the Media Manager database	44
7.4.2 Oracle specific information	47
Create tablespaces manually for Oracle RAC, Oracle ASM (Automated Storage Management)	47
Minimum Oracle privileges	47
Installing the Context module under Oracle 11g R2	49
Secure connection to Oracle	50
7.4.3 Microsoft SQL Server specific information	50
Operating the application without db_owner role	50
Operating the application without database user "OPASPUBLIC"	51
Installing full-text search for Microsoft SQL Server	52
Activating further iFilters on Microsoft SQL Server 2008	53
7.5 Supplier Portal Database	53
7.5.1 Download the Product 360 Supplier Portal install file	54
7.5.2 Create your Database Installation Root	54
7.5.3 Setup initial database by install script	54
Configure the database properties in the configuration.properties file	55
Execute Setup.cmd script	57
7.5.4 Alternatively: Setup custom database manually	59
Setup Oracle Schema	59
Setup MS SQL Schema	61
7.6 Audit Trail Database	63
7.6.1 Oracle RAC, Oracle ASM (Automated Storage Management)	63
7.6.2 Download the Audit Trail zip	64
7.6.3 Extract the Audit Trail archive	65
7.6.4 Configure the database properties	65
7.6.5 Install database:	66
Windows	66
Linux	66

8	Server Installation	67
8.1	Prerequisite	67
8.1.1	OS User Permissions	67
	Windows	67
	Linux	69
8.1.2	OS Volume Shares and Permissions	69
	Single Server.....	69
	Multi Server	69
8.1.3	Default Product 360 Server Ports	69
8.1.4	Encryption of secure information	70
	Usage of AES-256 cryptographic algorithm to encrypt/decrypt secure information	70
8.2	Control Center	71
8.2.1	First Node	71
	Download and Extract Binaries	71
	Configure Control Center.....	72
	Configure Application Server Cluster	73
	Install Control Center Service.....	74
	Validate Control Center Installation.....	76
8.2.2	Distribute Control Center on Remaining Nodes	76
8.3	Application Server	76
8.3.1	Binaries	76
8.3.2	Configuration.....	77
	General Server Settings (server.properties)	77
	Startup parameters (_environment.conf).....	79
	License	80
8.3.3	Installation.....	80
8.3.4	Enable Monitoring in Control Center.....	80
8.4	Validate Installation	80
8.5	Media Asset Provider	81
8.5.1	Media Manager Provider	81
8.5.2	Classic Provider	81
	GraphicsMagick for Classic Provider	81
9	Desktop Client Installation	82
9.1	Prerequisite	82

9.2	Binaries.....	82
9.3	Installing the client with MSI file.....	82
9.4	Starting the client.....	86
9.5	Single Sign-On.....	88
9.5.1	LDAP Authentication.....	88
9.5.2	SAML Authentication.....	89
10	Message Queue Installation.....	89
10.1	Prerequisites for the following products.....	89
10.2	Installing the Apache Message Queue 5.x.x.....	89
10.3	Run Apache Message Queue 5.x.x as a service.....	90
10.4	Enable the JMX for Apache Message Queue.....	90
10.5	Security (optional).....	91
10.6	Clustering(optional).....	92
11	Media Manager Installation.....	93
11.1	Prerequisite.....	93
11.2	Pre-Installation Checklist.....	93
11.2.1	OS User Permissions.....	93
	Windows.....	93
11.2.2	OS Volume Shares and Permissions.....	93
11.2.3	Default Product 360 - Media Manager Ports.....	93
	Port range.....	94
11.3	Media Manager Installation.....	95
11.3.1	Installation checklist.....	95
	New installation.....	95
	Update.....	95
11.3.2	Installing File Server.....	95
11.3.3	Installing Funcd.....	96
	General information.....	96
	File server Funcd.....	96
	Second Pipeline Funcd (optional).....	102
11.3.4	Installing the client modules.....	103
	Installing the client modules.....	103

Installing and setting up the ODBC connection under Macintosh	104
11.3.5 Installing the web front end	105
Windows	105
Linux	106
Encrypted passwords in configuration files	109
11.3.6 Setting up PIM - Media Manager	110
11.3.7 Installation - General aspects	110
General requirements	110
Installation - Linux	110
Installation - Windows	111
11.3.8 Configuration	111
General	111
Parameter configuration	112
More configuration options	114
11.3.9 Operation	114
Advanced configuration	114
Using own default images	115
Logging	116
11.4 Media Manager Integration	118
11.4.1 Product 360 - Server	118
Integrating Product 360 - Media Manager	118
11.4.2 Product 360 - Desktop Client	128
12 Supplier Portal Installation	128
12.1 Pre-Installation Checklist	128
12.1.1 OS User Permissions	128
Windows	128
Linux	128
12.1.2 Product 360 - Supplier Portal Default Ports	129
Change Application Server Ports	129
12.2 Supplier Portal Integration	130
12.2.1 Prerequisite	130
12.2.2 Setup Product 360 Core Users and Permissions	130
Create required Users and Groups within Product 360 - Desktop	130
Setup Product 360 - Web Users and Permissions for Product 360 Supplier Portal Item Editor/Viewer	132
12.2.3 Setup communication Product 360 Server - Product 360 Supplier Portal	136

12.3	Media Manager and Supplier Portal Integration	137
12.3.1	Prerequisite	137
12.3.2	Setup Hotfolder	137
12.3.3	Setup REST Service.....	141
	Tomcat and Java	141
	Installation HMM REST war	141
	Configuration HMM REST war	141
	Startup	142
12.4	Web and Supplier Portal Integration	142
12.4.1	Prerequisite	142
12.4.2	Configure Product 360 Supplier Portal Item Editor System User within Product 360 - Web	142
12.5	Server Installation on Windows.....	143
12.5.1	Prerequisite	143
12.5.2	Download the Product 360 Supplier Portal zip	143
12.5.3	Create Your Product 360 Supplier Portal Server Installation Root	143
12.5.4	Configuration.....	144
	Configure Product 360 Supplier Portal central configuration file.....	144
	Configure Logging	147
12.5.5	Install Tomcat	147
	Install Product 360 - Supplier Portal Tomcat Windows Service	147
	Start/Stop/Configure Product 360 - Supplier Portal Tomcat Windows Service	148
	(optional) Uninstall Product 360 - Supplier Portal Tomcat Windows Service.....	149
12.6	Server Installation on Linux	149
12.6.1	Prerequisite	149
	Java	149
12.6.2	Download the Product 360 Supplier Portal zip	150
12.6.3	Create Your Product 360 Supplier Portal Server Installation Root	150
12.6.4	Configuration.....	150
	Configure Product 360 Supplier Portal central configuration file.....	150
	Configure Logging	153
12.6.5	Install Tomcat	154
	Install Product 360 - Supplier Portal Tomcat Linux Service.....	154
	Start/Stop Supplier Portal Tomcat Server.....	154
	Deinstallation	155
12.7	Language Pack Installation	155

12.7.1	Overview	155
12.7.2	Installation.....	155
12.8	Installation Troubleshooting	155
13	Audit Trail Installation.....	157
13.1	Prerequisite	157
13.2	Pre-Installation Checklist.....	158
13.2.1	OS User Permissions	158
	Windows	158
13.2.2	Audit Trail Default Ports	158
13.3	Audit Trail Server Installation.....	158
13.3.1	Extract the Audit Trail archive	158
13.3.2	Configure the server connections.....	158
13.3.3	Configure the network configuration.....	159
13.3.4	Start Audit Trail server.....	161
	Windows	161
	Linux	161
13.4	Configure Audit Trail in the Product 360 Application	161
13.4.1	Enable Audit Trail	161
13.4.2	Message Queue Connection Configuration	161
13.4.3	ATCS local storage configuration.....	162
13.4.4	Further Configuration	163
13.4.5	Audit Trail network configuration	163
	Https connection between P360 server and Audit Trail server	163
	Multiple Audit Trail servers behind a load balancer	163
13.4.6	Start Product 360 Server	163
13.5	Activate Audit Trail for Entities in Repository	163
14	Business Process Management	163
14.1	Informatica BPM Installation	164
14.1.1	Informatica BPM Installation	164
	Installation of the Informatica BPM service.....	164
	Webserver and Java	164
	Post installation steps	164
	Integrated Security.....	166

14.2	BPM specific configuration within server.properties	168
14.2.1	Simple connectivity test	168
14.2.2	Service endpoints and partner links within Informatica BPM workflows.....	169
14.3	Failsafe handling of calls to Informatica BPM.....	170
15	Web Search Installation.....	171
15.1	Pre-Installation Checklist.....	172
15.1.1	System Requirements.....	172
	Memory Requirement	172
	Java	172
15.1.2	OS User Permissions	172
	Windows	172
	Linux	172
15.1.3	Web Search Default Ports	172
	Change Application Server Ports.....	172
15.2	Web Search Integration	173
15.2.1	Prerequisite	173
15.2.2	Setup Product 360 Permissions for Web Search	173
	Permission Settings for Product 360 - Web User to use Web Search.....	173
	Permission Settings for Product 360 - Desktop User to use Web Search Index Build	173
	Permission Settings for Technical Product 360 - Web Search REST User	173
15.2.3	Setup Configuration for Product 360 - Core.....	174
15.2.4	Setup Configuration for Product 360 - Web	174
15.3	Server Installation on Windows.....	175
15.3.1	Create Your MDM P360 - Web Search Server Installation Root.....	175
15.3.2	Setup Web Search Configuration.....	175
15.3.3	Web Container Password Hashing	178
	Disable Tomcats password authentication	179
15.3.4	Create Web Search Server Start Script and Web Search Windows Service Script	179
15.3.5	Start Web Search Server.....	179
15.3.6	Stop Web Search Server	180
15.4	Server Installation on Linux	180
15.4.1	Prerequisite	180
15.4.2	Installation.....	180
	Java	180

If you're not sure whether you have Java installed correctly:	181
If you need to install Java, follow these instructions:	181
Create the Product 360 - Web Search Server Installation Root	181
15.4.3 Configuration.....	181
Web Container Password Hashing	184
Disable Tomcats password authentication	185
Generate install/remove/start/stop script	185
15.4.4 Install Tomcat	185
Install Product 360 Web Search Tomcat Linux Service	186
Start/Stop Product 360 Web Search Tomcat Server./pim.....	186
Deinstallation	186
15.5 Installation Troubleshooting	186
16 Appendix.....	189
16.1 Language Packs.....	189
16.2 Standard Classification Systems.....	189
16.2.1 Download.....	190


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.

2 Pre-Installation Checklist

Before beginning to install, please check that:

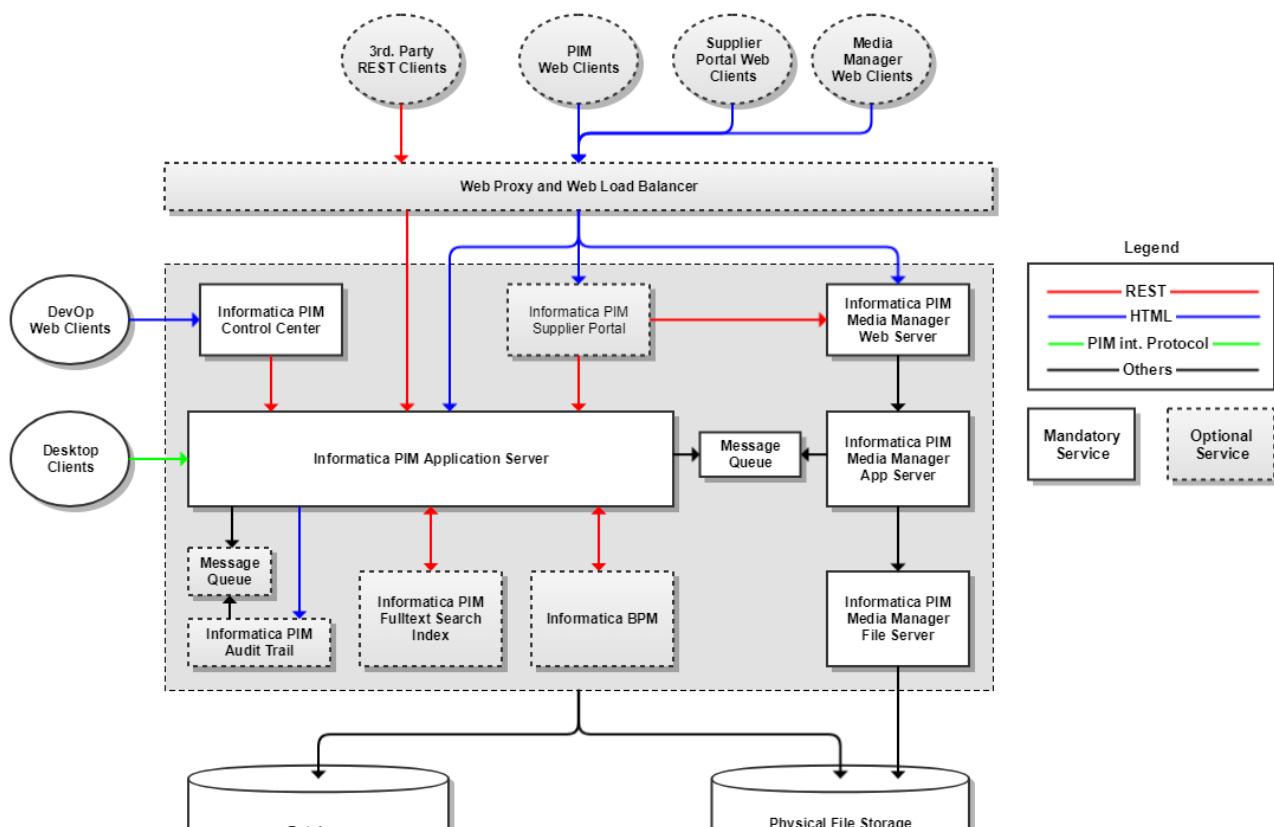
- Your system meets the requirements of the Product Availability Matrix (PAM)

 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.

3 Logical Service Overview

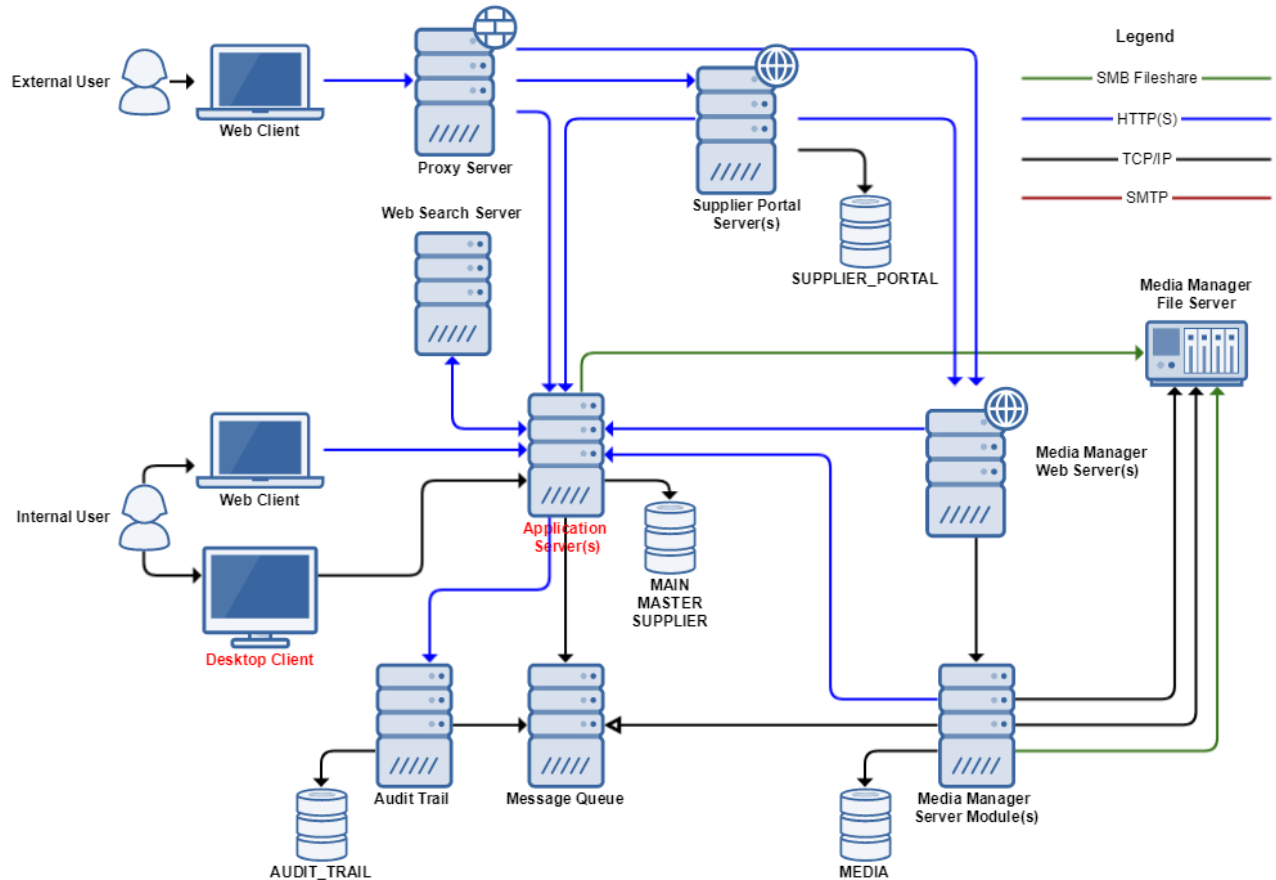
The following diagram gives a logical overview on the services which are involved in the overall Product 360 application. The deployment strategy should be individually defined based on the sizing requirements of the customer. Examples for a typical and full deployment can be found alter in this chapter.





4 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.



5 Port Overview

5.1 Database

Port	Database
1433	MSSQL
1521	Oracle

5.2 Server, Web and Desktop

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.
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.
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 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

5.3 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)
84	tcp	Product 360 - Media Manager Web XOB Connection (Data) (optional for Product 360 8 only for upgrade)

Port	Protocol	Product 360 Module
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

5.4 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
Hotfolder	7	59176	60671
Archive	8	59177	60672
Interface	9	59178	60673
Medias	11	59180	60675
Production	12	59181	60676
Administration	14	59183	60678

5.4.1 Supplier Portal

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

Port	Protocol	Product 360 Module
8080	http	Product 360 - Media Manager REST
1512	http	Product 360 - Server Service API

5.4.2 Audit Trail

Port	Protocol	Product 360 Module	Description
61616	tcp	MessageQueue	This port is used for sending messages from Product 360 Core to Product 360 - Audit Trail server over MessageQueue.
2801	http	HTTP port	This port is used for the communication between Product 360 - Server and Product 360 - Audit Trail server (for obtaining change informations which are then displayed in the P360 - Desktop Client)

5.4.3 Web Search

Port	Protocol	Product 360 Module / Description
18090	http	Product 360 - Search Server (Tomcat Application Server)
1512	http	Product 360 - Server Service API

6 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.

6.1 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.

6.1.1 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

6.1.2 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.

6.1.3 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>_OperationManual.pdf	✗
PIM_<version>_SizingManual.pdf	✗
ActiveVos Installation Manual (http://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp)	✓



6.1.4 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.

6.1.5 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	✗
Product 360 Audittrail	PIM_<version>_AuditTrail.zip, PIM_<Version>_ThirdPartySoftware.zip	✗
ActiveVos	ActiveVOS_Server_windows_9.2.4.exe	✓

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

6.2 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.

6.2.1 1. Installation of the Product 360 Server

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none"> PIM_<version>_Core.zip 	<ul style="list-style-type: none"> PIM_<version>_InstallationManual.pdf PIM_<version>_Installation_and_Operation.pdf PIM_<version>_ConfigurationManual.pdf (optional) 	---	

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.

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.

1.3 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.

6.2.2 2. Installation of the Product 360 Desktop Client

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none">• PIM_<version>_Core.zip	<ul style="list-style-type: none">• PIM_<version>_InstallationManual.pdf	<ul style="list-style-type: none">• 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.

6.2.3 3. Installation of the Product 360 Supplier Portal

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none">• PIM_<version>_SupplierPortal.zip• PIM_<version>_SupplierPortal_Languages.zip (optional)	<ul style="list-style-type: none">• PIM_<version>_InstallationManual.pdf	<ul style="list-style-type: none">• Product 360 Server• sqlplus or sqlcmd	

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*.

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*

6.2.4 4. Installation of Active Message Queue

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none">• PIM_<Version>_ThirdPartySoftware.zip	<ul style="list-style-type: none">• PIM_<version>_InstallationManual.pdf	---	<ul style="list-style-type: none">• for Product 360 Audittrail• for Product 360 Media Manager

The installation of the Active Message Queue has to be done if the Product 360 - AuditTrail or Product 360 - Media Manager will be installed. Otherwise this step can also be skipped. The installation of the Message Queue is described in detail in chapter 9.1 -9.6 *Message Queue Installation* of the *Installation Manual*.

6.2.5 5. Installation of Product 360 Audit Trail

Required installation file(s)	Required documentation	Required installations	Man dato ry
<ul style="list-style-type: none">PIM_<version>_AuditTrail.zip	<ul style="list-style-type: none">PIM_<version>_InstallationManual.pdf	<ul style="list-style-type: none">Active Message QueueProduct 360 ServerProduct 360 Desktop client	

5.1 Installation of the database

Before installing the Product 360 Audit Trail server, the database has to be installed. There is a detailed installation guide of how to install the database in the *Installation Manual* chapter 6.6.1 - 6.6.5 *Audit Trail Database*.


5.2 Installation of Audit Trail

After installing the database, the Audit Trail server can be installed. The detailed Installation guide can be found in the *Installation Manual* in chapter 12.3.1 - 12.3.4 *Audit Trail Installation*.

5.2.1 Configure Product 360 Server and Client to enable Audit Trail

By default the Audit Trail feature is disabled for Product 360 server. Chapter 12.4.1 - 12.4.6 *Configure Audit Trail in the Product 360 Application* describes how the Audit Trail can be enabled for server and client.

6.2.6 6. Installation of BPM / ActiveVos

Required installation file(s)	Required documentation	Required installations	Ma n dato ry
ActiveVOS_Server_windows_9.2.4.exe	<ul style="list-style-type: none">PIM_<version>_InstallationManual.pdfhttp://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp?nav=%2F3_0	<ul style="list-style-type: none">Product 360 ServerA Tomcat Application Server 7.x or 8.xA JDK 1.7 or 1.8JDBC 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.

6.1 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 use 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.

6.3 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.

6.2 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.

6.3 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.

6.4 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.

6.5 Installation of Active Vos

Run ActiveVOS_Server_windows_9.2.4.exe and follow the installation wizard. The installation 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_deploy.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/> .

6.6 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*.

6.2.7


7. Installation of Websearch

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none">PIM_<version>_WebSearch.zip	<ul style="list-style-type: none">PIM_<version>_Installation Manual.pdf	<ul style="list-style-type: none">Product 360 ServerProduct 360 Desktop ClientProduct 360 Web Client	

7.2 Installation of Websearch

The websearch doesn't need any database install and also the Tomcat application server is provided within the package. A detailed installation guide is provided in the Installation Manual at chapter 15 Web Search Installation.

6.2.8 8. Installation of Product 360 Media Manager

Required installation file(s)	Required documentation	Required installations	Mandatory
<ul style="list-style-type: none">• PIM_<version>_MediaManager.zip• PIM_<version>_MediaManager_Languages.zip• PIM_<version>_ThirdPartySoftware.zip	<ul style="list-style-type: none">• PIM_<version>_Installation Manual.pdf	<ul style="list-style-type: none">• Product 360 Server	

8.1 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*.

8.2 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*.

7 Database Installation

7.1 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](#) which should support you with the important points in matter of the Product 360 database installation.

7.1.1 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

7.1.2 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

7.1.3 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

7.2 DBMS Installation and Configuration Hints

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.

7.2.1 Microsoft SQL Server

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

Server Settings

Maximum Degree of Parallelism (MAXDOP)

Please limit the database MAXDOP to 2 (cost = 50) as Product 360 is a high transaction OLTP application.

Number of TempDB Files

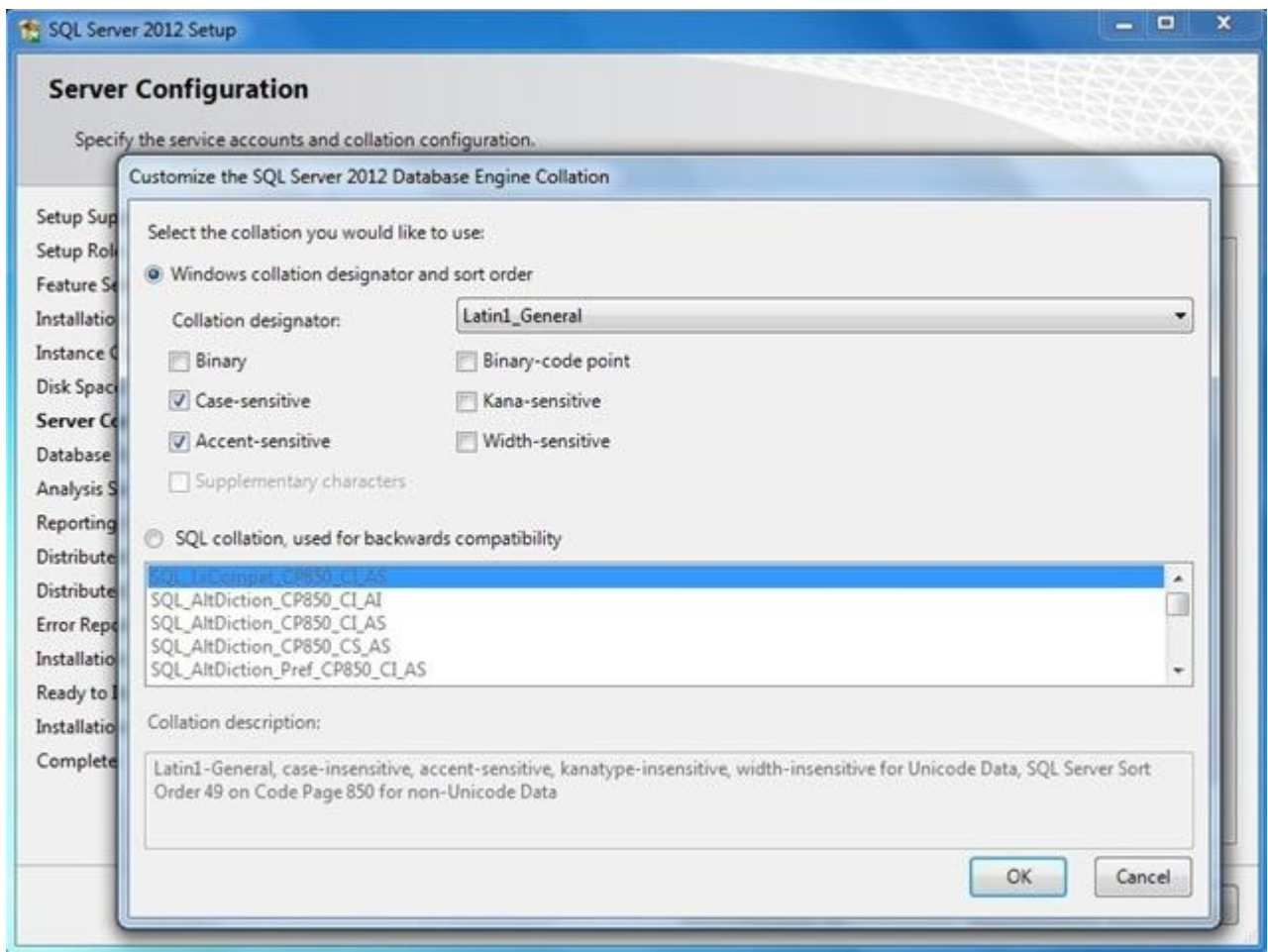
Since all Product 360 Schemas/Databases use the SNAPSHOT isolation mode of SQL Server a high temp DB throughput is required. We recommend to have a tempdb file for each physical CPU core (till up to 8 files).

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

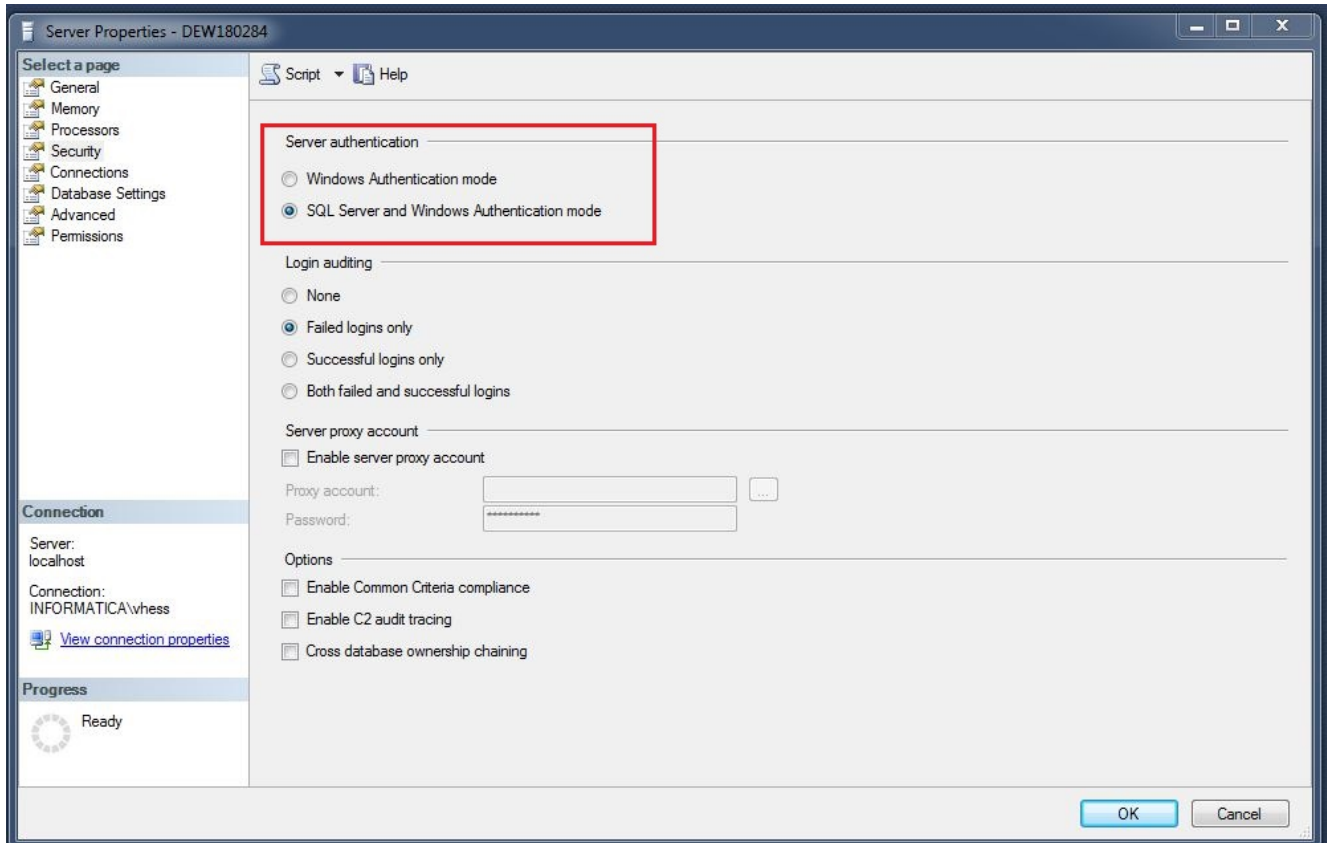
Screenshot: SQL Server Management Studio 2012 login properties dialog



! 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.



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



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

7.2.2 Oracle

Consider these settings during installation of the database instance.

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 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 expiration, otherwise ensure that passwords for Product 360 schemas never expire
- Ensure have enough space for TEMP tablespace

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 too 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_cache_size	2000M	Reduces additional overhead on dynamic allocation.
db_domain		
db_file_multiblock_read_count	<ensure parameter is not set>	To be determined automatically by Oracle.
db_writer_processes	CPU cores / 8	Oracle guideline.
disk_asynch_io	TRUE	Oracle guideline.
dynamic_sampling	2	To enable dynamic sampling on tables without statistics (ReportStore/ReportStoreTemp).

Name	Value	Description
filesystemio_options	ASYNCH	
java_pool_size	0	To be determined automatically by Oracle.
large_pool_size	400M	If undefined, RMAN would use the SHARED POOL.
job_queue_processes	10	
memory_target	2/3rd of available memory	
memory_max_target	2/3rd of available memory	
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	
processes	1000	Sufficient Oracle processes are allocated to support connection, parallel thread, internal process and other usage.
recyclebin	OFF	

Name	Value	Description
remote_logi n_passwordf ile	EXCLUSIVE	
sessions	1000	
sga_target	2/3rd of max_memor y	
shared_pool _size	400M	We recommend 400Mb to start. Increase this in line with the value seen in the Oracle AWR report for this instance taken under typical heavy load Section: Cache Sizes > Shared Pool Size
undo_manage ment	AUTO	
tns_listene r	TCP Protocol	
workareas_s ize_policy	AUTO	To be determined automatically by Oracle.

Database User Settings

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

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

7.3 Server Database




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

7.3.1 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.

7.3.2 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

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 likely 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";
```

7.3.3 Minimum Oracle privileges

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 user 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	-

System Privileges	Granted	Admin
CREATE TABLESPACE	X	-
CREATE SEQUENCE	X	-
CREATE TABLE	X	-
CREATE PROCEDURE	X	-
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 ;
```

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 users have to be created before the installation process by an Oracle DBA. See chapter ["Oracle RAC, Oracle ASM \(Automated Storage Management\)"](#).

The database user 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 ;
```

7.3.4 Binaries

The database setup is distributed within the product core archive and has the following format
PIM_<Version>_<Revision>_dbSetupClient_win32.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.

Extract the database setup archive

On the database server extract the PIM_<Version>_<Revision>_dbSetupClient_win32.zip to an installation root of your choice.

For this documentation we will choose C:\INFORMATICA\PIM (= <PIM_DATABASE_INSTALLATION ROOT>)

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](#) in the [Server Installation](#) 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 Oracle TCPS connection for P360 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_win32.zip\configuration\server.properties.template.[DBMS]` to `server.properties`
2. Adjust the settings as described in the following table:

Property	Description
General Settings	
<code>repository.default.language</code>	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 <code>server.properties</code> 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!)	
<code>db.integrated.security</code>	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.
<code>db.default.type</code>	This property should never be changed!
<code>db.default.server</code>	The host name of the Microsoft SQL Server
<code>db.default.port</code>	Port of the Microsoft SQL Server instance, usually this is 1433
<code>db.default.user</code>	User name of the database user (if integrated authentication is used this property can be empty)

Property	Description
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
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
db.default.data.size.growth	<p>Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs</p> <div>  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! </div>
db.default.log.size	Default size in MB allocated for a database transaction log file; adapt this setting to your needs
db.default.log.size.growth	<p>Default increment value in MB allocated when space for a database transaction log file is insufficient; adapt this setting to your needs</p> <p>Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs</p> <div>  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! </div>

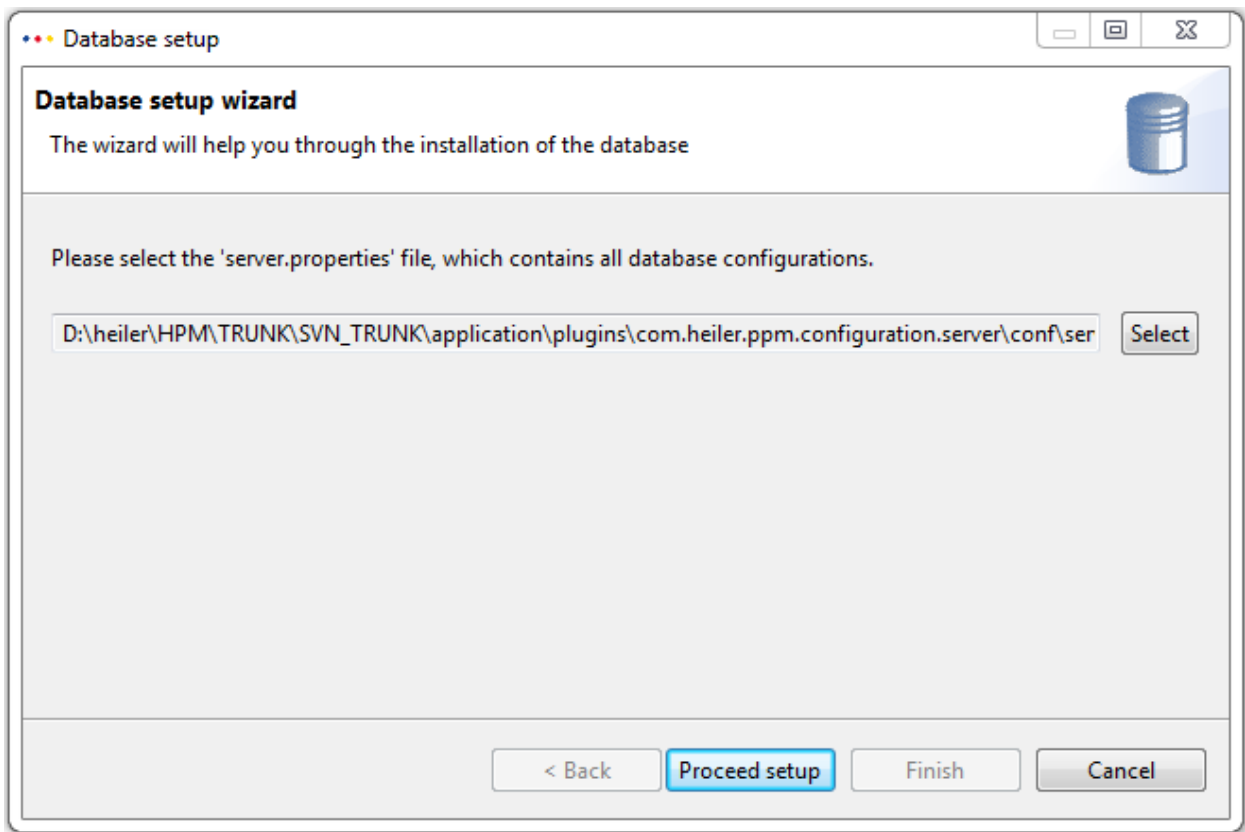
Property	Description
db.default.schema.prefix	Usually, this property needs not to be changed. The common prefix for all server schemas; it must be in capital, start with a latin character and must not contain any special characters except '_'!
db.default.schema.suffix	Usually, this property needs not to be changed. The common suffix for all server 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.
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	Never change this property!
db.default.database	Oracle Service Name
db.default.server	The host name of the Oracle 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
db.default.dir.data	Folder for the database schema files

Property	Description
db.default.dir.tmp	Folder for the database transaction log files
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	<p>Default increment value in MB allocated when space for a database schema is insufficient; adapt this setting to your needs</p> <div>  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! </div>
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	<p>Default increment value in MB allocated when space a transaction log file is insufficient; adapt this setting to your needs</p> <div>  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! </div>
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	<p>Default increment value in MB allocated when space for an index tablespace is insufficient; adapt this setting to your needs</p> <div>  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! </div>
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 '_'!
db.default.schema.suffix	<p>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 '_'!</p> <p>This property is helpful to distinguish between productive and test schemas (e.g. _PRO and _TEST).</p>
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	<p>Affects the default prefetch size which is especially important for mass data retrieval.</p> <p>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.</p> <p>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).</p>

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.

Database setup

Database setup wizard

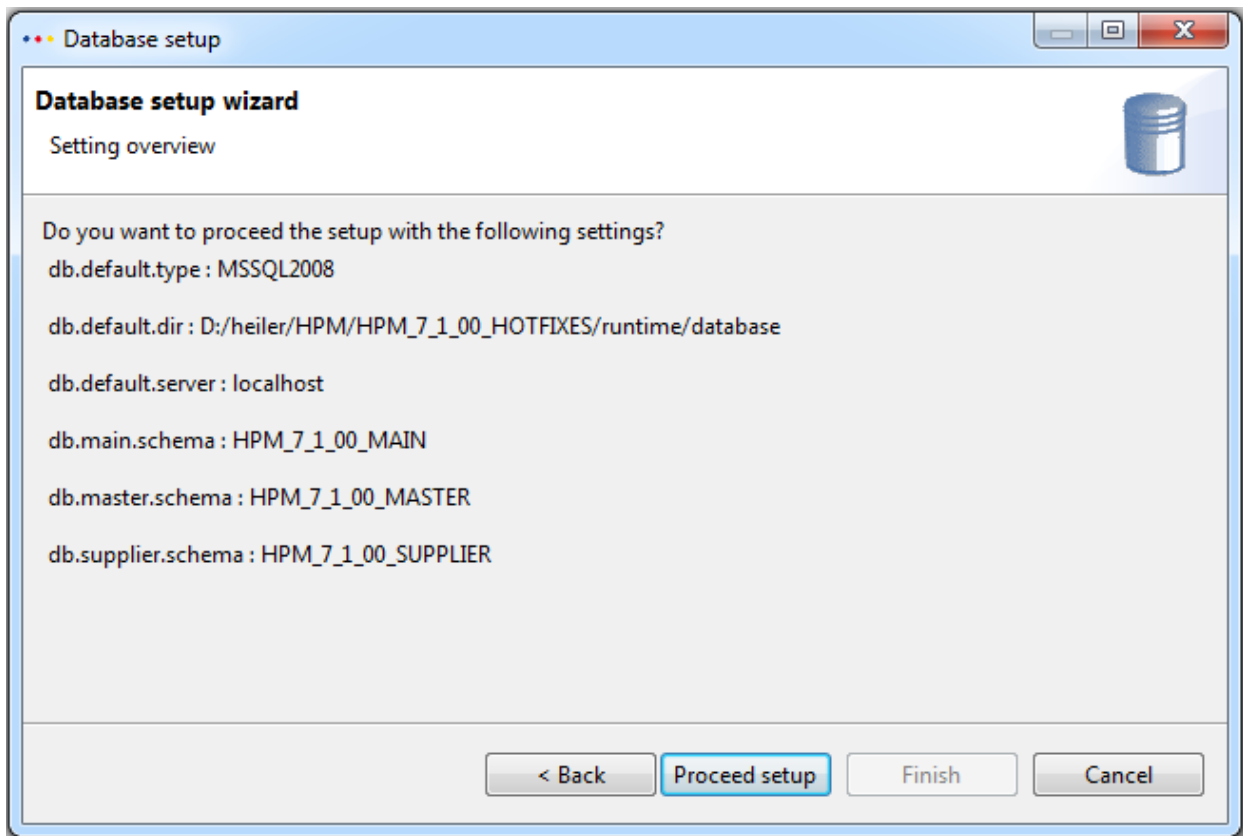
Please enter the login data for an system user

User

Password

< Back Proceed setup Finish Cancel

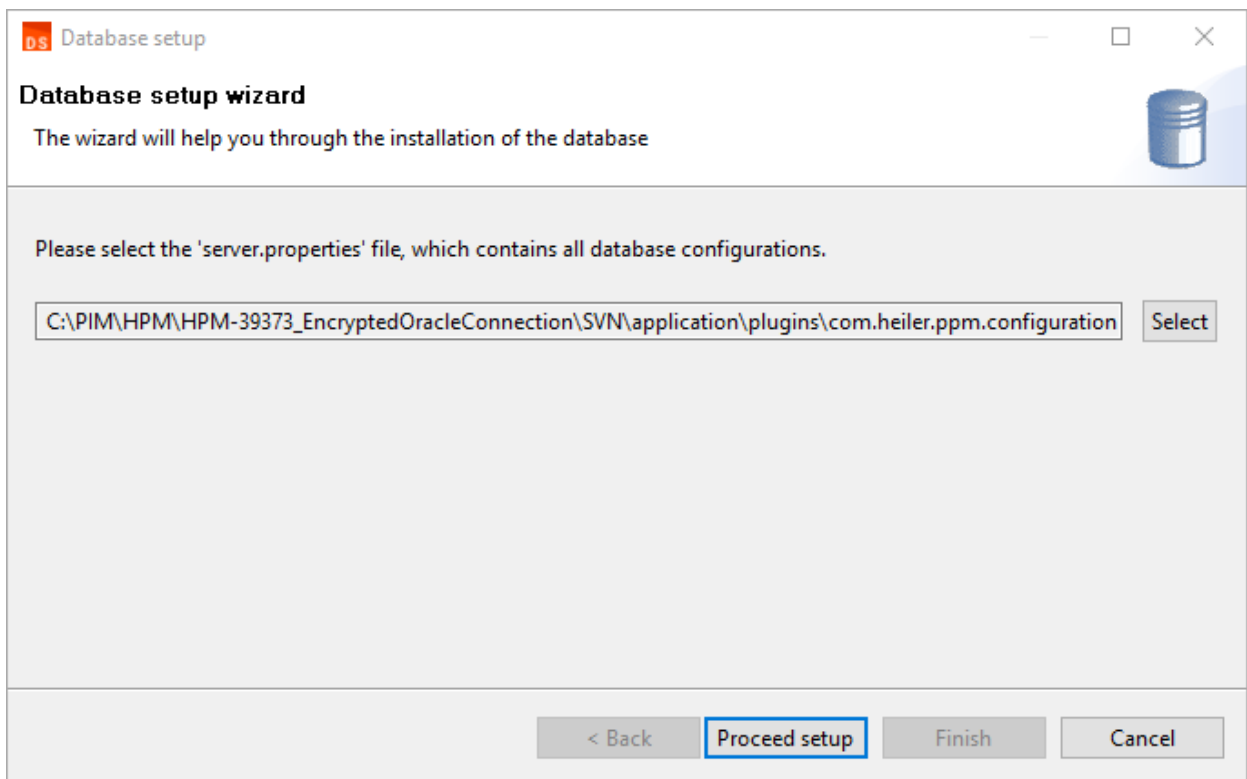
4. After clicking Proceed setup you will get an overview of some settings of the server.properties file you selected.



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 were 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.

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 whether you want to use a TCP or a TCPS connection.

Database setup

Database setup wizard

Please enter the login data for an system user

User:

Password:

Protocol:

< Back Proceed setup Finish Cancel

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

Database setup

Database setup wizard

Setting overview

Do you want to proceed the setup with the following settings?

db.default.type : ORA11g

db.default.database : TLS

db.default.dir : E:/oracle11_2_0_4_0/HPM1/TLS

db.default.server : HSQS200

db.main.schema : HPM_MAIN

db.master.schema : HPM_MASTER

db.supplier.schema : HPM_SUPPLIER

< Back Proceed setup Finish Cancel

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 were 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.

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 parameter.
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 in 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.

7.3.5 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 occurs we can not guarantee a consistent state of the database.**

7.4 Media Manager Database

7.4.1 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](#)) 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

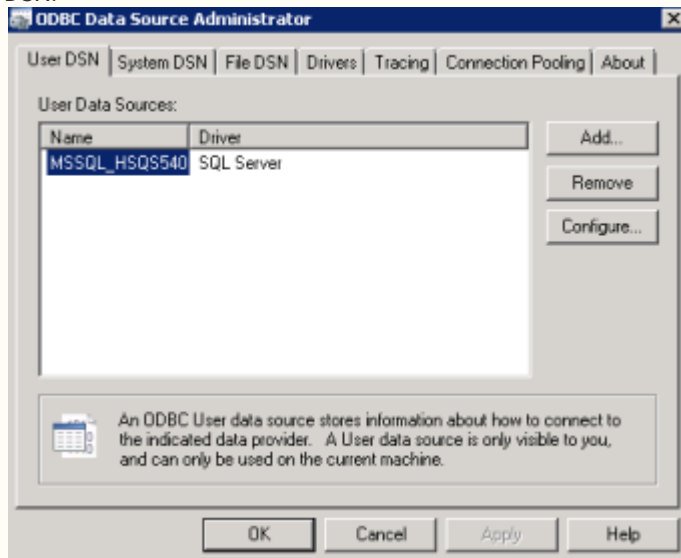
Please make sure that you installed the Oracle instant client software to connect to an existing oracle database. The easiest way to install this software is to install the Product 360 - Media Manager modules (see: [Installing the client modules](#)).

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](#). This will skip the table space creation process in installation program and start the content installation directly.

9. You may now change the password for Product 360 - Media Manager database user OPASUSER.
10. Oracle only: 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.

7.4.2 Oracle specific information

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/opasing.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;
```

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	-

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

Installing the Context module under Oracle 11g R2

To install the Context module under Oracle 11g R2, carry out the steps described below:



The installation under Windows or Solaris only differs in terms of the path separators.

- As the value of the environment variable **ORACLE_SID** set your Oracle instance with the following command:
 - Windows: **set ORACLE_SID=SID_Your_Instance**
 - Unix: **ORACLE_SID=SID_Your_instance # export ORACLE_SID**
- Launch SQLPlus with the following command: **sqlplus "/" as sysdba**
- Remove the user ctxsys with the following command: **sqlplus> DROP USER CTXSYS CASCADE;**
- Call up the file catctx.sql using your administrator password:
 - Windows: **sqlplus> @%ORACLE_HOME%\ctx\admin\catctx password OPASIMG TEMP FALSE;**
 - Unix: **sqlplus> @\$ORACLE_HOME/ctx/admin/catctx <password> OPASIMG TEMP FALSE;**
- Set file_acces_role to public: **sqlplus> exec ctxsys.ctx_adm.set_parameter('file_access_role','public');**
- Give the user OPASUSER additional rights: **sqlplus> GRANT CTXAPP TO OPASUSER; sqlplus> GRANT RESOURCE TO OPASUSER; sqlplus> GRANT CONNECT TO OPASUSER;**
- Complete the transaction: **sqlplus> COMMIT;**
- Exit SQLPlus: **sqlplus> quit;**
- Launch SQLPlus and log in as ctxsys with the corresponding password: **sqlplus ctxsys/password**
- Run the script drdefd.sql:
 - Windows: **sqlplus> @\$ORACLE_HOME\ctx\admin\defaults\drdefd.sql;**
 - Unix: **sqlplus> @\$ORACLE_HOME/ctx/admin/defaults/drdefd.sql;**
- Exit SQLPlus: **sqlplus> quit;**
- Switch to the directory **/Manual/ORACLE Installation/ContextCartridge/11g** of the uncompressed archive..
- Launch SQLPlus: **sqlplus opasuser/opaspass**
- Run the script Create_11g.sql: **sqlplus> @Create_11g.sql; [****]**
- Exit SQLPlus: **sqlplus> quit;**

This completes installation of the Context module.

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.

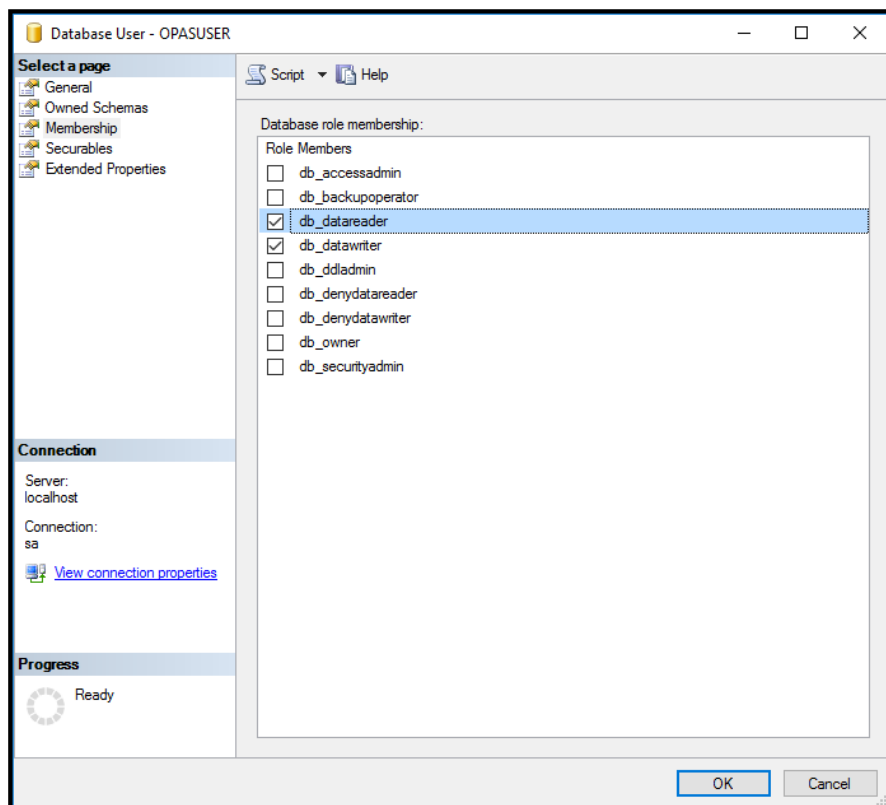
7.4.3 Microsoft SQL Server specific information

The minimum privileges for the user which installs the database are:

Permission	With grant
ALTER ANY LOGIN	-
CONNECT SQL	-
CREATE ANY DATABASE	-
VIEW ANY DATABASE	-
VIEW SERVER STATE	X

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. Please do not remove this role until at least one IMM module was started (e.g. Administration).

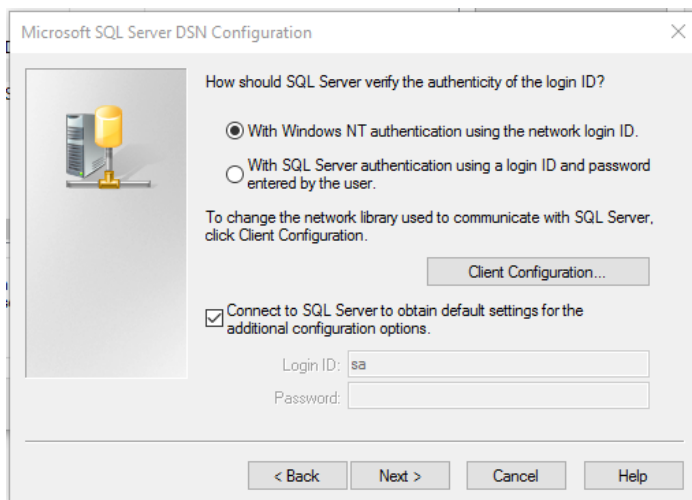
Operating the application without database user "OPASPUBLIC"

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 against your company policy you have the possibility to work with domain accounts. How to configure 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 manual for example in the SQL server management studio the application will not work.

The screenshot shows the 'Modify system data' window with the 'Standard' tab selected. Key fields include:

- Unique company code:** A text field with the value 'MSDEMC'.
- Path info of Informatica Media Manager Volume 0:** A text field with the value 'V:\localhost\PIM_Share\Volume0'.
- Settings for modules in automatic mode:** A section with a checkbox 'No automatic re-logon of an automatic module from' and time fields '00:00' and '00:00'.
- Local Informatica Media Manager settings:** A section with a 'Macro player' field.
- Presettings:** A section with checkboxes for 'Use detailed security prompts when deleting?' and 'Activation of LDAP login'. It also includes fields for 'Max. number of table entries to be displayed in lists' (200), 'Currency unit' (USD), and 'Usage number range'.
- LDAP settings:** A section with a checkbox for 'Activation of LDAP login'.

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
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.

- 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.

- Mark **Tables** at the Object Explorer and click on the **Refresh** button.
- Mark the F_IMGKONT table at the Object Explorer and choose **Full-Text index > Define Full-Text Index** at the context menu.
- The wizard for installing the full-text search opens.
- Click on **Next**.
- At the first step the PK_F_IMGKONT index is already chosen; click on **Next**.
- At the second step mark the PKONT_CONTENT column by clicking at the check box on the left.
- Choose PKONT_EXT under the **Type** Column.
- Click on **Next**.
- At the third step leave the setting on **Automatically** and click on **Next**.
- 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.)
- Click on **Next**.
- At the fifth step, click on **Next** without any changes.
- At the last step you see a summary; click on **Finish**.
- 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.
- 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.

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.

- Open the Microsoft SQL Server Management Studio.
- Log on as administrator (user sa).
- Open a new query.
- 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'**

7.5 Supplier Portal Database

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.

7.5.1 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.

7.5.2 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

7.5.3 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**.

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 <div>  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. </div>
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 successful 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.

Execute Setup.cmd script

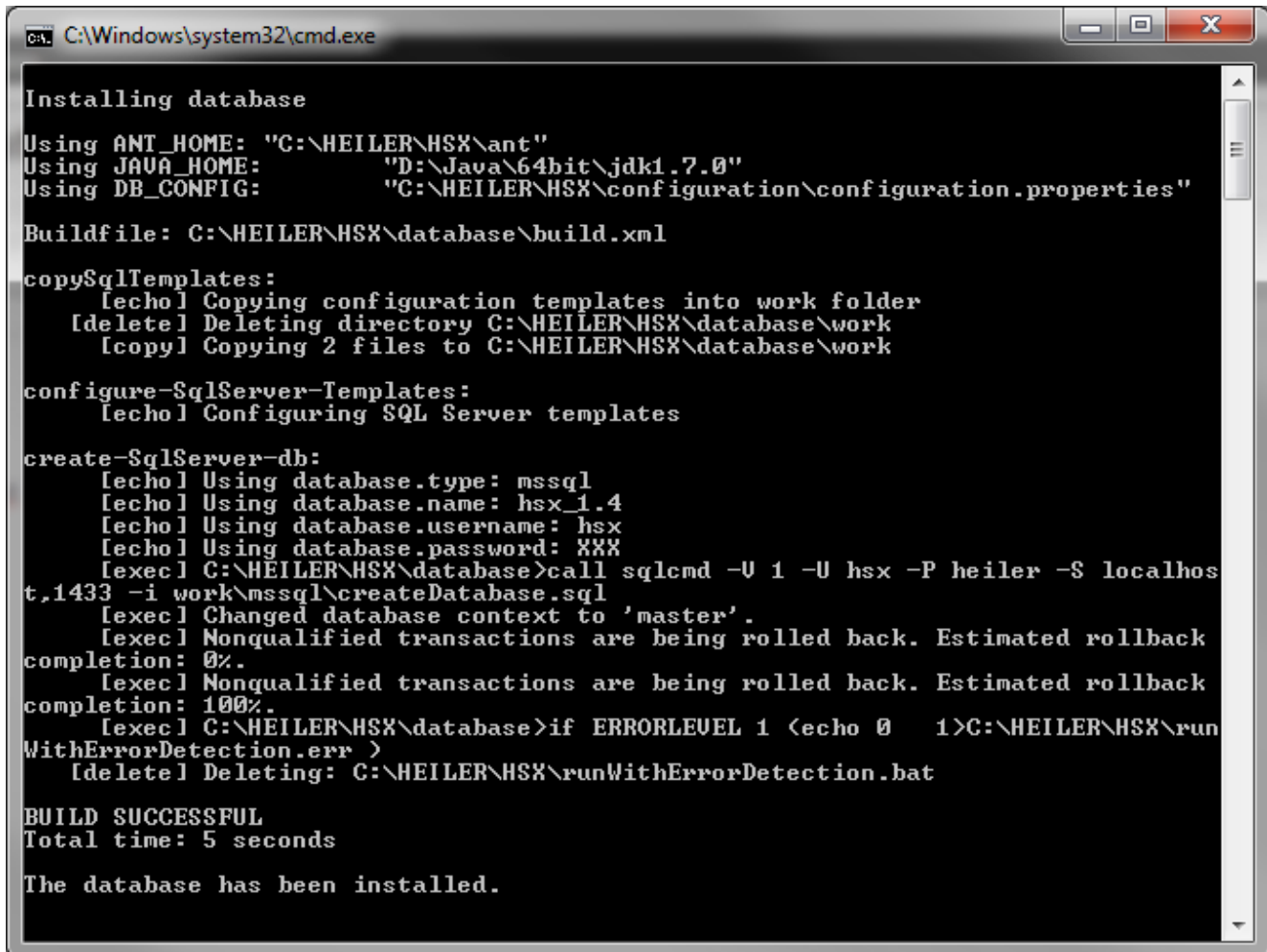
The database scripts are executed using ANT. The SQL template files can be found in /database/templates/mssql/createDatabase.sql and /database/templates/oracle/createDatabase.sql.

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](#) 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



```
C:\Windows\system32\cmd.exe

Installing database
Using ANT_HOME: "C:\HEILER\HSX\ant"
Using JAVA_HOME: "D:\Java\64bit\jdk1.7.0"
Using DB_CONFIG: "C:\HEILER\HSX\configuration\configuration.properties"
Buildfile: C:\HEILER\HSX\database\build.xml

copySqlTemplates:
[echo] Copying configuration templates into work folder
[delete] Deleting directory C:\HEILER\HSX\database\work
[copy] Copying 2 files to C:\HEILER\HSX\database\work

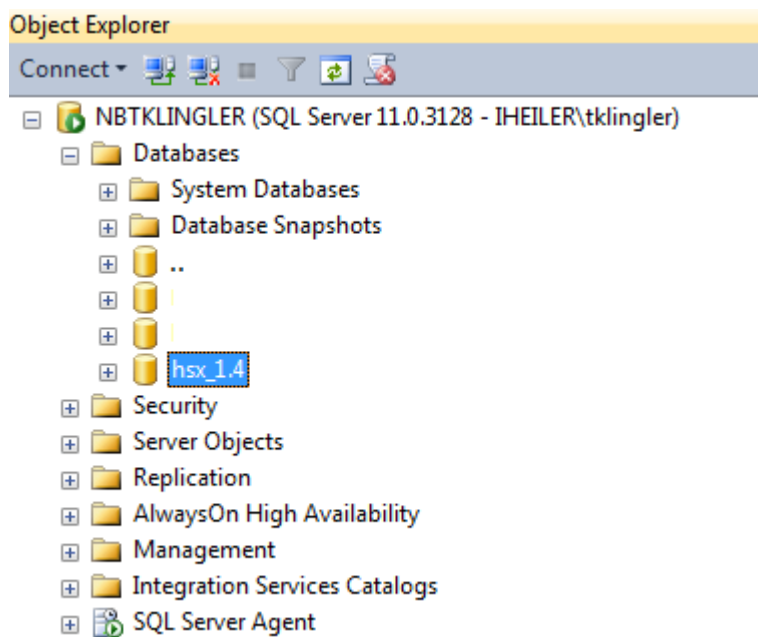
configure-SqlServer-Templates:
[echo] Configuring SQL Server templates

create-SqlServer-db:
[echo] Using database.type: mssql
[echo] Using database.name: hsx_1.4
[echo] Using database.username: hsx
[echo] Using database.password: XXX
[exec] C:\HEILER\HSX\database>call sqlcmd -U 1 -U hsx -P heiler -S localhost,1433 -i work\mssql\createDatabase.sql
[exec] Changed database context to 'master'.
[exec] Nonqualified transactions are being rolled back. Estimated rollback completion: 0%.
[exec] Nonqualified transactions are being rolled back. Estimated rollback completion: 100%.
[exec] C:\HEILER\HSX\database>if ERRORLEVEL 1 (echo 0 1>C:\HEILER\HSX\runWithErrorDetection.err )
[delete] Deleting: C:\HEILER\HSX\runWithErrorDetection.bat

BUILD SUCCESSFUL
Total time: 5 seconds

The database has been installed.
```

Screenshot: SQL Server Management Studio 2012 showing created database

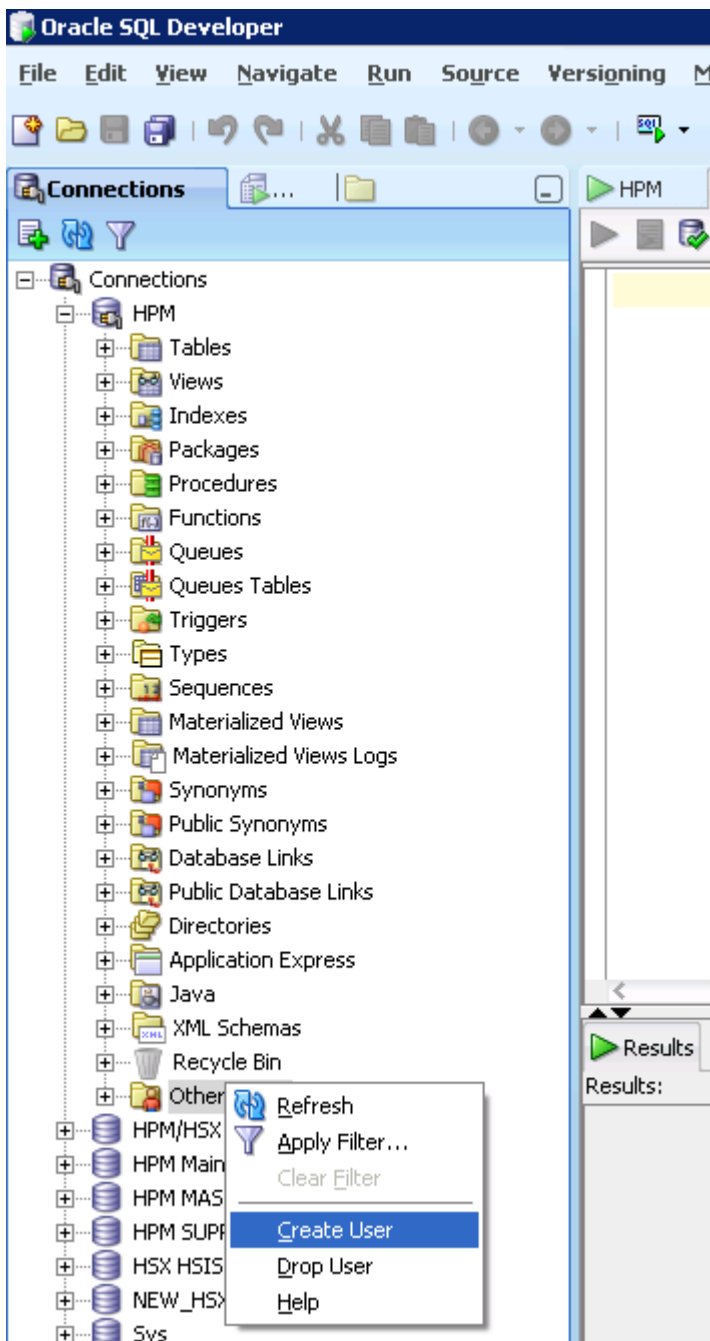


7.5.4 Alternatively: Setup custom database manually

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

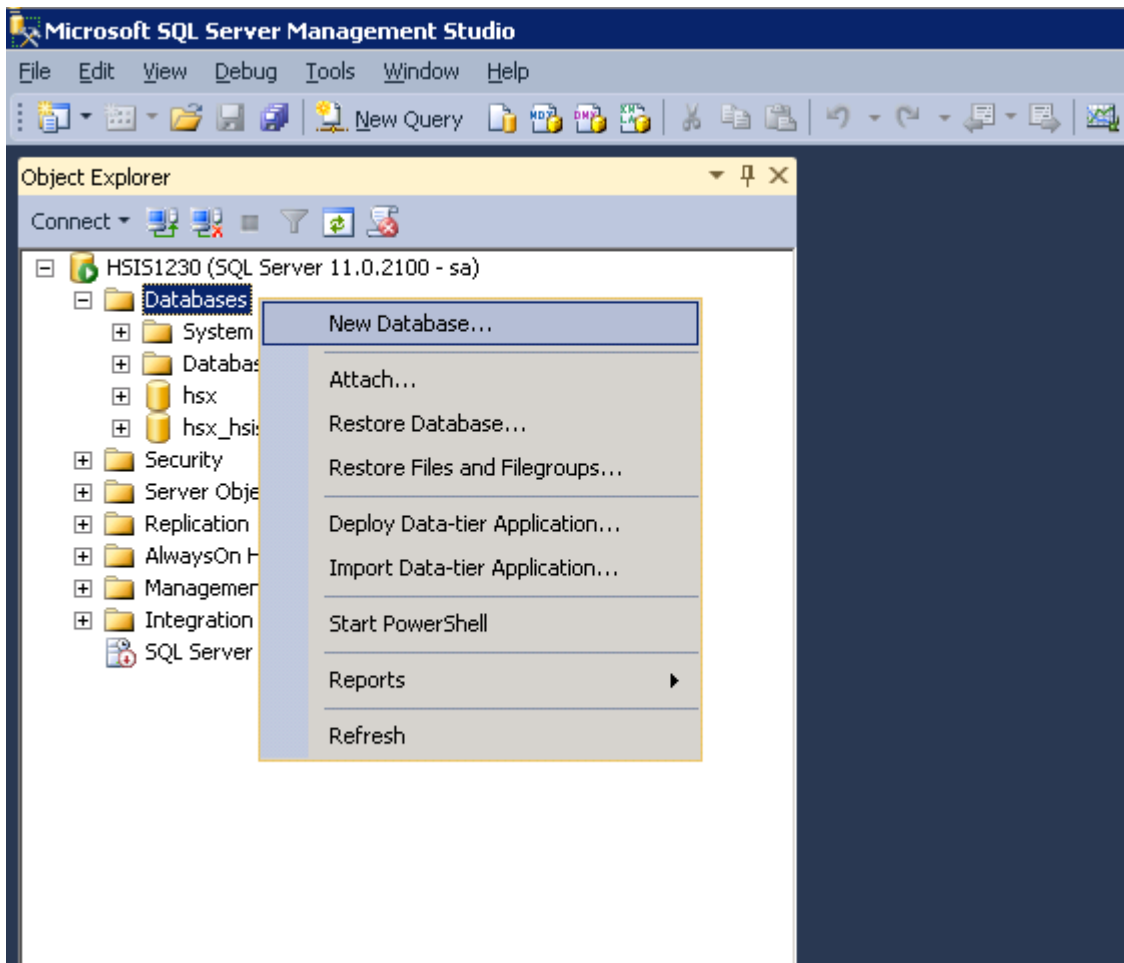
By default, the user password expires after a certain period of time. To disable password expiration you will have to execute the following lines:

```
alter profile default limit password_life_time unlimited;
```

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_COMMITTED_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.

7.6 Audit Trail Database



The [Audit Trail Database](#) manual describes how to initially setup or update the Product 360 server database schemas for a new release.

Audit Trail needs its own data storage. It is strongly recommended to deploy the product 360 Core database and Audit Trail database on different servers or at least on different storage. This is necessary because the Audit Trail database requires a lot of disk space and fast I/O.

7.6.1 Oracle RAC, Oracle ASM (Automated Storage Management)

Please note that the audit trail 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

Prefix (db.default.schema.prefix)	Schema Name	Suffix (db.default.schema.suffix)	Username	Temp Tablespace	Data Tablespace	Index Tablespace
PIM_	AUDITTRAIL		PIM_AUDITTRAIL	PIM_AUDITTRAIL_TEMP	PIM_AUDITTRAIL_DATA	PIM_AUDITTRAIL_INDEX

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

Example: MAIN Script

```

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

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

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

CREATE USER "PIM_AUDITTRAIL"
PROFILE "DEFAULT"
IDENTIFIED BY pimadmin
DEFAULT TABLESPACE "PIM_AUDITTRAIL_DATA"
TEMPORARY TABLESPACE "PIM_AUDITTRAIL_TEMP"
ACCOUNT UNLOCK;

GRANT UNLIMITED TABLESPACE TO "PIM_AUDITTRAIL";
GRANT "CONNECT" TO "PIM_AUDITTRAIL";
GRANT "RESOURCE" TO "PIM_AUDITTRAIL";

```

7.6.2 Download the Audit Trail zip


To obtain the download package for Audit Trail please raise a Shipping Request with Informatica.

7.6.3 Extract the Audit Trail archive

Choose your <ARCH> version and unpack the corresponding audit trail server archive **PIM_<Version>_<Revision>_atserver<ARCH>.zip** (windows) or **PIM_<Revision>_atserver<ARCH>.tgz** (Linux) to an installation root <**PIM_AUDITTRAIL_INSTALLATION_ROOT**> (for example C:\INFORMATICA\PIM\AuditTrail).

7.6.4 Configure the database properties


 There should be no white space in the <**PIM_AUDITTRAIL_INSTALLATION_ROOT**> otherwise setup will fail.

 If you want to encrypt the database passwords in the configuration file please refer to chapter [Encryption of secure information](#) in the [Server Installation](#) manual. The passwords marked as to encrypt will be encrypted during the database setup.

Before running the database installation, some basic configuration needs to be done.

1. Go to <**PIM_AUDITTRAIL_INSTALLATION_ROOT**>/configuration/audittrailserver/
2. Rename server.properties.template.MSSQL2008 or server.properties.template.ORA11g file to **server.properties**
3. Update database connection properties if necessary (defaults assume you have database instance running on localhost)

Database settings	
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.audittrail.server	Hostname of the database server
db.audittrail.port	Port number of the database server
db.audittrail.dir.local	Local directory at database server to store files which are related to Audit Trail
db.audittrail.schema	Database/Schema name in capital letters
db.audittrail.user	Database username. For Oracle database users same as schema If Microsoft SQL Server "Integrated Security" is in use, set to empty
db.audittrail.password	Password for the above specified database user If Microsoft SQL Server "Integrated Security" is in use, set to empty

 Configured directory (db.audittrail.dir.local) should exist otherwise database setup will fail.

Database settings (Oracle only)	
db.sys.password	Update password for SYS user that should be with SYSDBA role. It's required for installation and can be removed after
db.audittrail.tns	The TNS name used by Oracle. Please verify that TNS is enabled at Oracle Database

7.6.5 Install database:



For installation on Oracle db, please make sure that sqlplus is installed and working on the machine where you execute the install script

Windows

1. Go to **<PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin**
2. Run **setup_console.bat** in folder **<PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin**
3. A console with **osgi>** prompt pops up, press return after log4j message
4. Type **dbinstall** in console and confirm installation.
5. After installation check out **<PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/dbsetup/*.log**
If it was successful there will be all following log files without failures expect **<databasename>_chek.log**.

script	
createsp_HPM_AUDITTRAIL_DEMO.txt	1 KB
HPM_AUDITTRAIL_DEMO_chek.log	1 KB
HPM_AUDITTRAIL_DEMO_create.log	1 KB
quotedidentifiers_HPM_AUDITTRAIL_DEMO.txt	0 KB
sysusercheck.log	0 KB
update_db.log	0 KB
updatescript_HPM_AUDITTRAIL_DEMO.txt	1 KB

Linux

1. Open terminal and navigate to the root of the installation package **<PIM_AUDITTRAIL_INSTALLATION_ROOT>**
2. Execute the command **bin/setup_console.sh**. If a file is not marked as executable, you have to mark it as executable with the command **chmod +x filename.sh**
3. An **osgi>** prompt will appear
4. Type **dbinstall** and confirm installation.
5. After installation check out **<PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/dbsetup/*.log**

6. If it was successful there will be all following log files without failures expect <databasename>_chek.log.

```
[root@InvgNCDPIMLOK001 dbsetup]# ls -ltr
total 36
drwxr-xr-x 3 root root 4096 Mar 11 19:05 script
-rw-r--r-- 1 root root 246 Mar 11 19:05 tns-connect.log
-rw-r--r-- 1 root root 228 Mar 11 19:05 HPM_AUDITTRAIL_chek.log
-rw-r--r-- 1 root root 6184 Mar 11 19:05 HPM_AUDITTRAIL_create.log
-rw-r--r-- 1 root root 140 Mar 11 19:05 HPM_AUDITTRAIL_get_updates.sql
-rw-r--r-- 1 root root 301 Mar 11 19:05 HPM_AUDITTRAIL_updatescript.txt
-rw-r--r-- 1 root root 2114 Mar 11 19:05 HPM_AUDITTRAIL_update.log
-rw-r--r-- 1 root root 900 Mar 11 19:05 HPM_AUDITTRAIL_createsp.log
```

8 Server Installation



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

8.1 Prerequisite

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

- [Product 360 Core Database](#)

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

Windows

The user who installs the MDM Product 360 needs to have local administrative permissions. **Also the service user for the Control Center needs to be an administrator on all cluster nodes, otherwise he will not be able to automatically install the application server services there.**

Create Control Center Service User

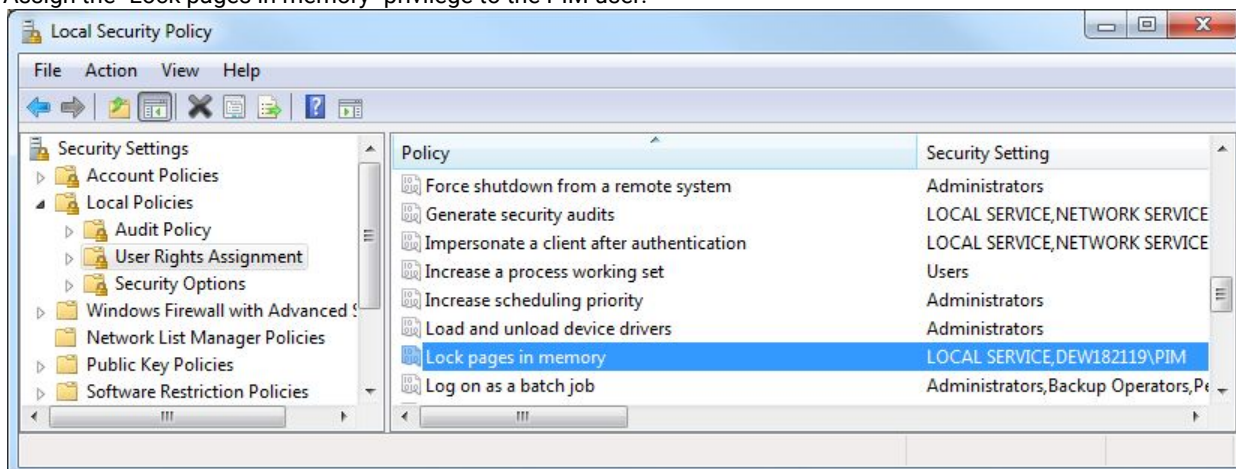
- Open Start > All Programs > Administrative Tools > Computer Management > Local Users and Groups > Users > New User ...

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



In case the host machines are part of a domain, we recommend to use a special domain user for the following steps, rather than creating your 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.



Linux

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

Create Control Center 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 using Control Center.

8.1.2 OS Volume Shares and Permissions

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.

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.
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)

Port	Protocol	Product 360 Module
1812	tcp	Data Grid communication. Needed for the synchronization heartbeat of the cluster. <div>  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. This 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. </div>
5555	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 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

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="Administrator"
password="[_to_encrypt_]MyPassword[_to_encrypt_]" />
</network>
```

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 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.



Usage of strong cryptographic algorithms to encrypt/decrypt secure information

Due to import control restrictions of some countries, the JCE policy that are bundled in the Java 8 Runtime Environment allow "strong" but limited cryptography is used by default. This means if you want to use a strong cryptographic algorithm like AES-256 you will need to change the configuration in file `<PIM ROOT>\server\jre\lib\security\java.security`. Enable the property 'crypto.policy=unlimited' to activate the unlimited cryptographic algorithms. Otherwise you will run into errors during encryption/decryption in Product 360, saying you're using an illegal key size.

Also after update to newest Hotfix the Java JCE 'java.security' file must be replaced in corresponding `jre\lib\security` folders of all Product 360 components.

8.2 Control Center

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.

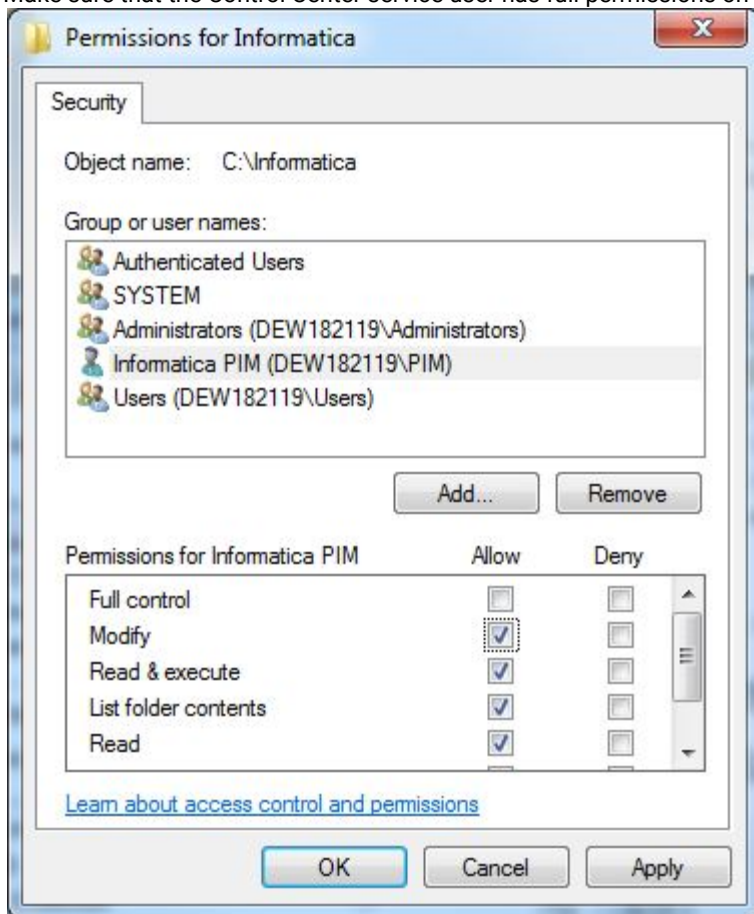
The Control Center must be installed on **every node** in the cluster. We strongly recommend to install all nodes absolutely identical, this prevents deployment failures and is the fastest way to setup the cluster.

8.2.1 First Node

Download and Extract Binaries

- Select one of your servers in the cluster to be the first node of your system. The installation will be done on this node and after that copied to all other nodes.
- Extract the Control Center package `PIM_8.0.5.00_<revisionNumber>_clusterix_win64.zip` resp. `PIM_8.0.5.00_<revisionNumber>_clusterix_linux64.tgz` from the Core archive
- Extract the file on the master node into a directory, e.g. `C:\Informatica\PIM (= <PIM ROOT>)`. The directory structure should look like this: `<PIM ROOT>\clusterix` and **not** like this `<PIM ROOT>\PIM_8.0.5.00_<revisionNumber>_clusterix_win64\clusterix`

- Make sure that the Control Center service user has full permissions on the <PIM ROOT> and all children.



Configure Control Center


! If you want to encrypt the passwords used in the configuration files please refer to chapter [Encryption of secure information](#) in the [Server Installation](#) manual. The passwords marked as to encrypt will be encrypted during the start of Control Center service.

Open the file <PIM ROOT>\clusterix\configuration\clusterix\ClusterixConfig.xml in an editor and adjust the properties as described below.

! **Note**
This file will be copied during "Update Configuration" process to PIM Server configuration folder and port and clusterixLogin will be used for communication from PIM Server to Control Center.

Property Name / Attribute	Description	Example
port	The HTTP port which should be used for the Control Center Web UI.	9000

Property Name / Attribute	Description	Example
clusterixHttpsConfiguration		
enabled	Enables HTTPS for Control Center Web UI.	false
httpsPort	The HTTPS port which should be used for the Control Center Web UI.	443
keyStoreFile	The full path to the keystore file.	D:/Development/ com.heiler.ppm.communication2/ testdata/keystore.jks
keyStorePassword	The password of the keystore file.	
clusterixLogin		
user	The username which must be used for access to the Control Center.	clusterix
password	The password to use for the Control Center.	
hpmLogin		
user	The username of the Product 360 user which has Service API access permissions. This user is not needed for the installation process, but later for monitoring Product 360 operations.	rest
password	The password of the Product 360 user.	

 Important Notice: When using HTTPS for the Control Center, make sure that your certificate is trusted! To do so follow these steps:

- export your certificate from your wanted keystore file by using this command in your java home path:
keytool -export -keystore fullPathToYourKeystoreFile -alias yourChosenAlias -file certificateName.cer
- import your exported certificate into the cacerts file at `yourJREHomePath\lib\security` by using the following command: **keytool -keystore cacerts -importcert -alias yourChosenAlias -file certificateName.cer**
- restart your system


=> to simplify this process, you can use an external tool named "portecle".

Configure Application Server Cluster

Open the file <PIM ROOT>\clusterix\configuration\clusterix\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.

Element/Attribute	Description	Example/ Default
network	Root element of the network configuration, contains one or more nodes	

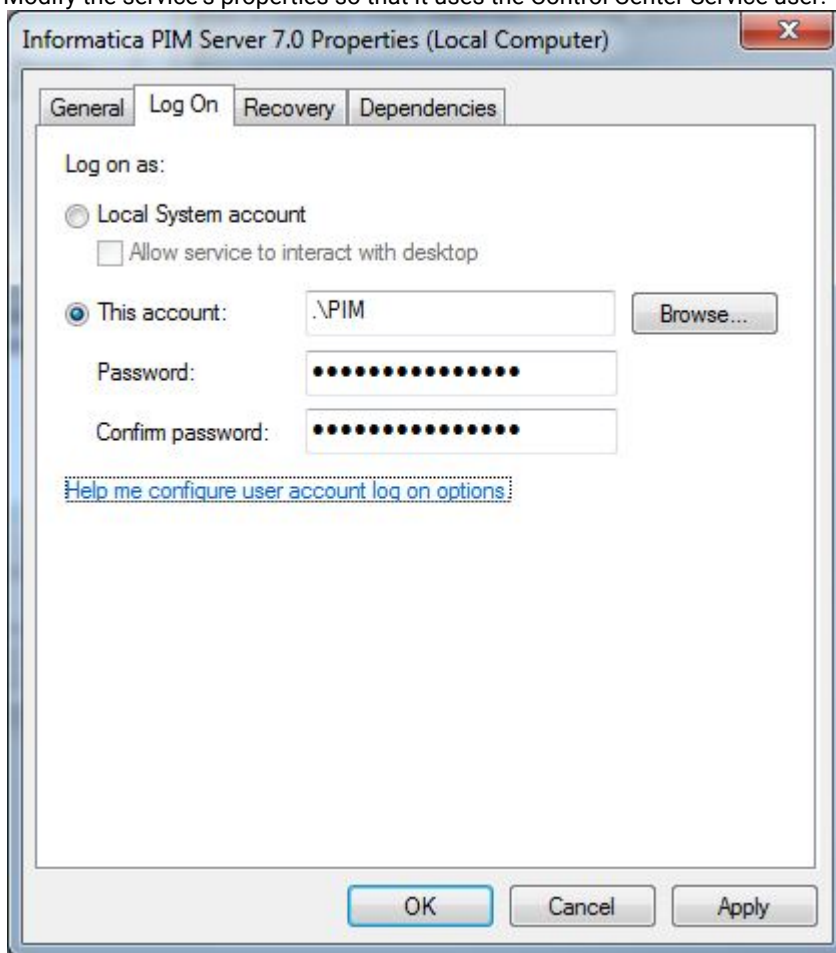
node	Represents a server node in the cluster	
identifier	Unique identifier of the node within the network. See <i>-Dppm.nodeIdentifier</i> command line argument below!	product360-server1
host	The host name / IP address this node runs on. Note: Do not use localhost or similar addresses. The host name 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	Default role(s) each server node must have at start time. Available roles are CLIENTS_SERVER and JOB_SERVER. Currently the server roles can not be modified during runtime of the server, but this might change in the future.	CLIENTS_SERVER and JOB_SERVER
<div>  <div>mandatory attribute</div> </div>		
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...

Install Control Center Service

Windows

- Install Control Center as service by running the script <PIM ROOT>\clusterix\install.cmd

- Open Start > All Programs > Administrative Tools > Services
- Make sure that the startup type is "Automatic"
- Modify the service's properties so that it uses the Control Center Service user.



- Start the service Informatica Product 360 Control Center

Linux

- If you do not want to run the Control Center as root you have to edit the script `<PIM ROOT>/clusterix/service/clusterix.sh` and change the line
`#RUN_AS_USER=`
to
`RUN_AS_USER=<USERNAME>`
whereby `<USERNAME>` is the name of the Control Center Service User
- Install Control Center as service by running the script `<PIM ROOT>/clusterix/install.sh`
- Start the service Informatica Product 360 Control Center by starting the service via
`service Product_360_ControlCenter_1.0 start`

Validate Control Center Installation



Note

Make sure that JavaScript is enabled in your browser. Currently Internet Explorer is not supported with the Control Center.

- Verify the installation of Control Center by opening the web interface on the first node (usually `http://<ServerName>:9000`). Replace 9000 with the port you used in the ClusterixConfig.xml. Login with the user name and password specified in the ClusterixConfig.xml file.
- Click on the Monitoring tab and open the Network tree to the left. Check that the all configured nodes of the cluster are shown under Application Server
- The web interface with two configured nodes should look like this:

Identifier	Server-Types	State	Host	CPU	Cores	Memory/Max (MB)	Disk Space/Max (GB)	Additional Informatic
suv12qa03	PIM_SERVER	RUNNING	SUV12QA03	5%	2	2512 / 3686	40.369 / 66.652	Running Jobs: 11
suv12qa04	PIM_SERVER	RUNNING	SUV12QA04	2%	2	1604 / 3686	33.868 / 66.652	Running Jobs: 1

8.2.2 Distribute Control Center on Remaining Nodes

- Copy the folder `<PIM_ROOT>\clusterix` of the first node to each remaining node of the cluster (including all the configurations which should be identical on all machines).
- Install and start the Control Center service on each machine (like described above).
- Validate the installation on each of the machines by opening the Control Center web interface

8.3 Application Server

8.3.1 Binaries

Extract the server installation package from the Core download archive. The package name is

`PIM_8.0.5.00_<revisionNumber>_server_win64.zip` resp. `PIM_8.0.5.00_<revisionNumber>_server_linux64.tgz`.



Hint

Do **not** unzip the

PIM_8.0.5.00_<revisionNumber>_server_win64.zip resp. PIM_8.0.5.00_<revisionNumber>_server_linux64.tgz file!

8.3.2 Configuration

All configuration for the application servers must be done only on one node and will automatically be distributed to all other nodes in the cluster.



If you want to encrypt the passwords used in the configuration files please refer to chapter [Encryption of secure information](#) 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 Oracle TCPS connection for P360 Server" in the "Server Configuration" manual.


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.

General Server Settings (server.properties)

File: <PIM_ROOT>\clusterix\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 <i>all servers</i> can access the <i>same file storage</i> and the <i>same directories</i> 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	

Property	Description
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)
Repository Settings	
repository.default.language	<p>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.</p> <div>  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. </div>
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	<p>If your security guidelines do not allow passwords in configuration files this preference allows you to use integrated authentication on Windows operating systems.</p> <p>"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.</p>
db.default.server	<p>The host name of the Microsoft SQL Server;</p> <p>Change this in case you have a separate database server</p>
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	<p>Base folder for the database schema and database transaction log files (also used by the database setup)</p> <p>Note: This folder needs not to be local to the application server but to the database server!</p>
db.default.schema.prefix	<p>Usually, this property needs not to be changed. The common prefix for all Product 360 - Server schemas; it must be in capital and start with a latin character</p>

Property	Description
db.default.schema.suffix	Usually, this property needs not to be changed. The common suffix for all Product 360 - Server schemas; it must be in capital, and start with a latin character This property is helpful to distinguish between productive and test schemas (e.g. _PRO and _TEST)
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.database	Oracle 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, used by the database setup too Note: This folder needs not to be local to the application server but to the database server.
db.default.schema.prefix	The common prefix for all Product 360 - Server schemas; it must be in capital letters!
db.default.schema.suffix	The common suffix for all Product 360 - Server schemas; it must be in capital letters! This property is helpful to distinguish between productive and test schemas (e.g. _PRO and _TEST).

Startup parameters (_environment.conf)

File: <Product 360 ROOT>\clusterix\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
GC_THREADS	Set the parameter to the maximum number of concurrent garbage collection threads. You should not configure more than about 75% of the number of available CPU Cores.	e.g. 36 for a 48 Core machine

Parameter	Description	Default/Example
	NAME_SHORT, NAME_LONG, JMX_PORT and SERVER_IDENTIFIER will be adjusted automatically by the Control Center during the installation with the settings specified in the configuration files of Control Center.	

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.

8.3.3 Installation

- Open the Control Center Interface using your local browser. Connect to the node on which you adjusted the application server configurations.
- Open the Deployment tab.
- In the "Installation Files", press the upload button and select the application server archive. The archive has to stay zipped. Click on upload to upload the installation file.
- After the upload has been completed, select the application server archive in the widget and press the **Install** button.
The installation process will automatically copy the installation archive to all server nodes.
The archive will be extracted to `<PIM_ROOT>\server`.
Configuration files will be copied and adjusted accordingly.
Finally, the Windows/Linux service will be installed on the remote machines.
- If the Control Center service user does not have sufficient rights to install a service you have to 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
- Switch to the Monitoring tab and select the server(s) you want to start. Press the **Start Server** button.
The Server States will move from STOPPED to STARTING and finally RUNNING



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 for the Control Center service and make sure that this user has full access on the file share.

8.3.4 Enable Monitoring in Control Center

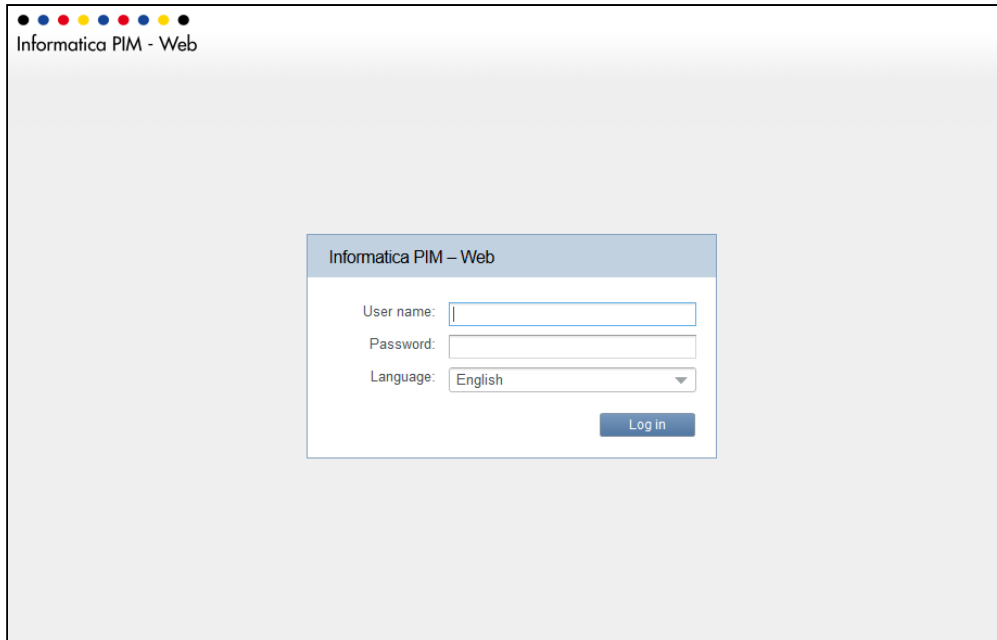
To be able to see all the statistical data for all servers you need to have a user in your Product 360 system who has Service login permissions and all process planning permission.

You can create this user using the Desktop Client. The user name and password should have been already defined in the `ClusterixConfig.xml` file, make sure the new user has the same name and password.

8.4 Validate Installation

When you finished the installation of a single server (or a cluster), you can easily validate if everything is up and running by opening the Informatica Product 360 Web interface.

By default, the web client is reachable via the following url: `http://hostName:1512/pim`




8.5 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 its 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.

8.5.1 Media Manager Provider

Please see separate instruction for the [Media Manager Integration](#)

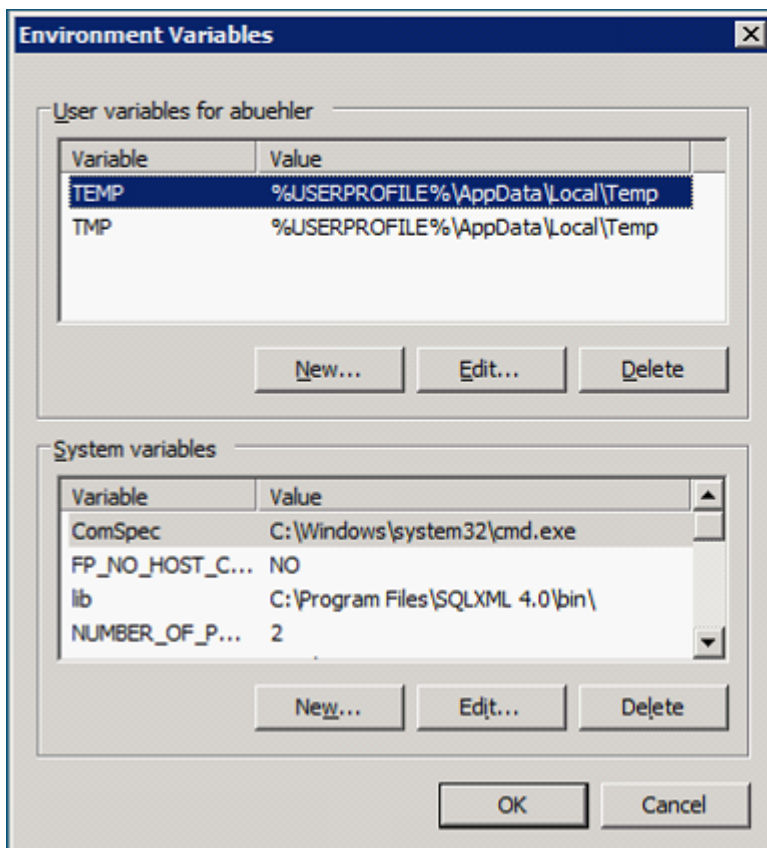
8.5.2 Classic Provider

 The Classic Provider is only supported for Windows operating system!

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 its 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

i This page describes the installation of the Informatica Product 360 Desktop Client

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.

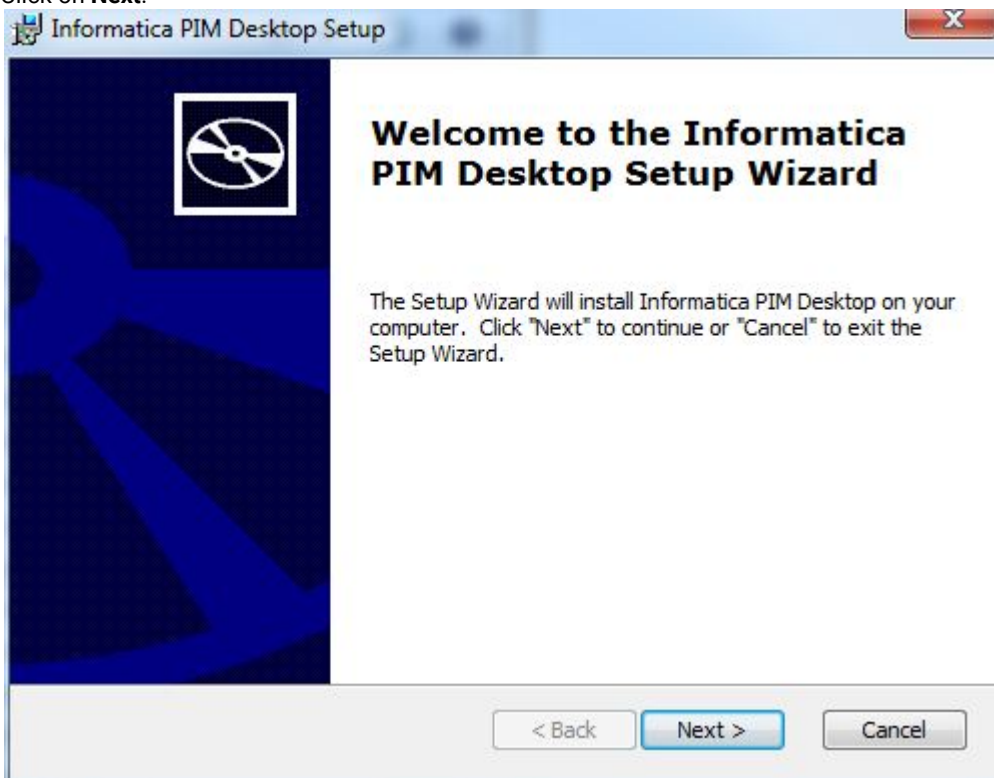
The client archive is distributed within the Product 360 core archive and has the following format `PIM_<Version>_<Revision>_client_win64.msi`

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.

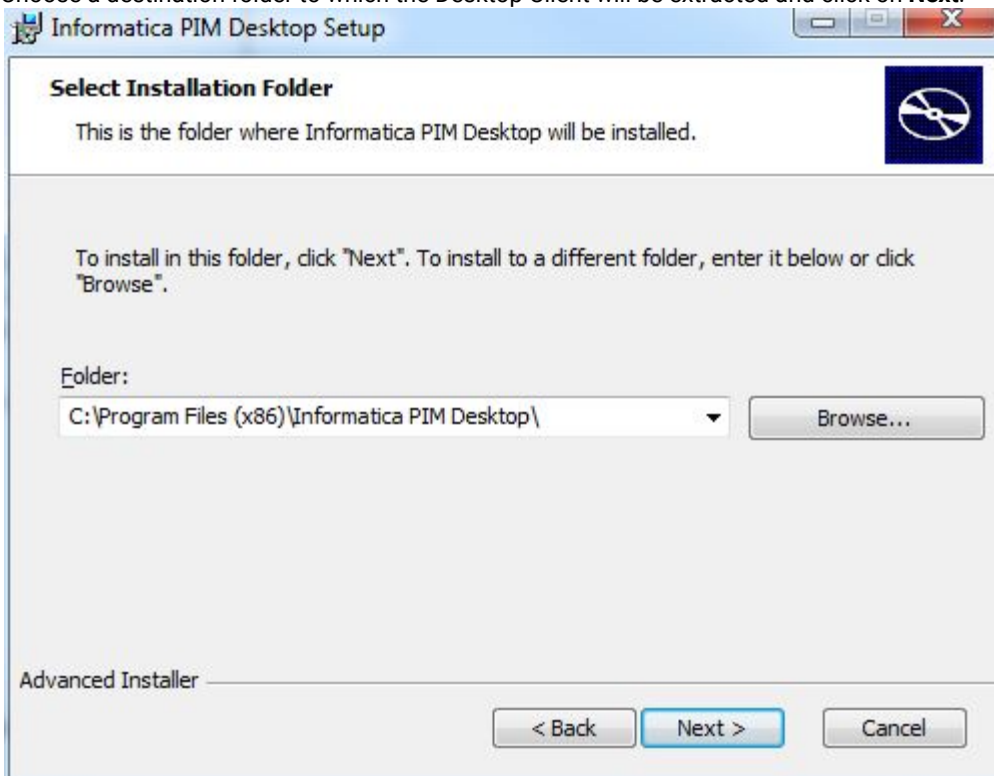
Perform the following steps:

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**.



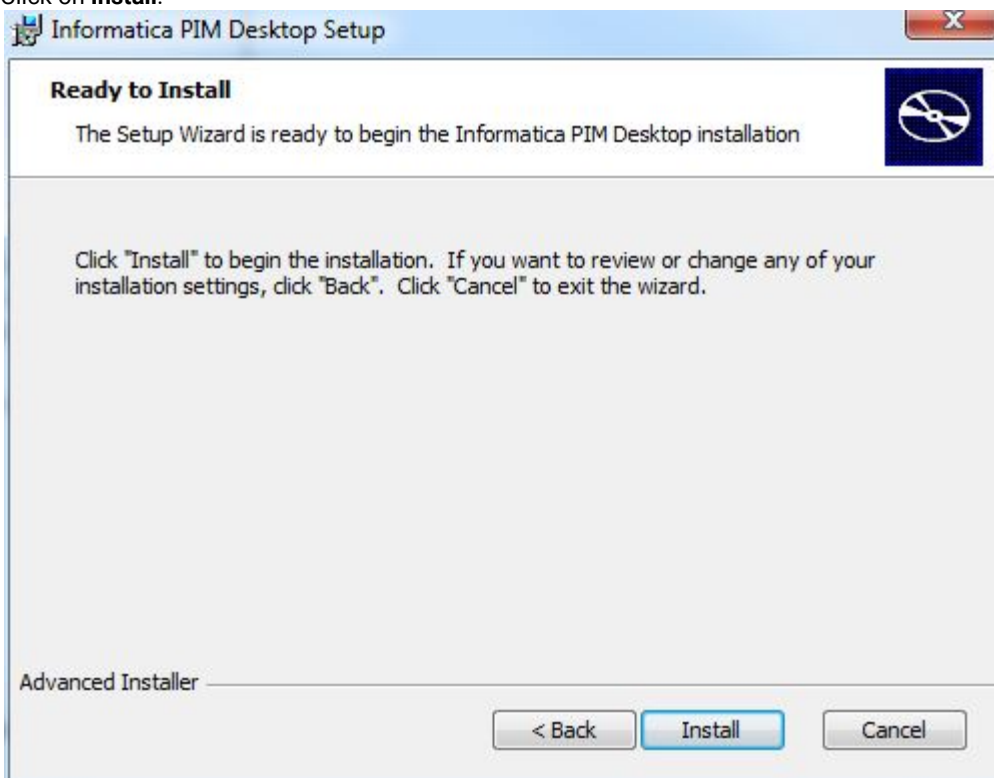
Welcome screen of Informatica Product 360 - Desktop Setup Wizard

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



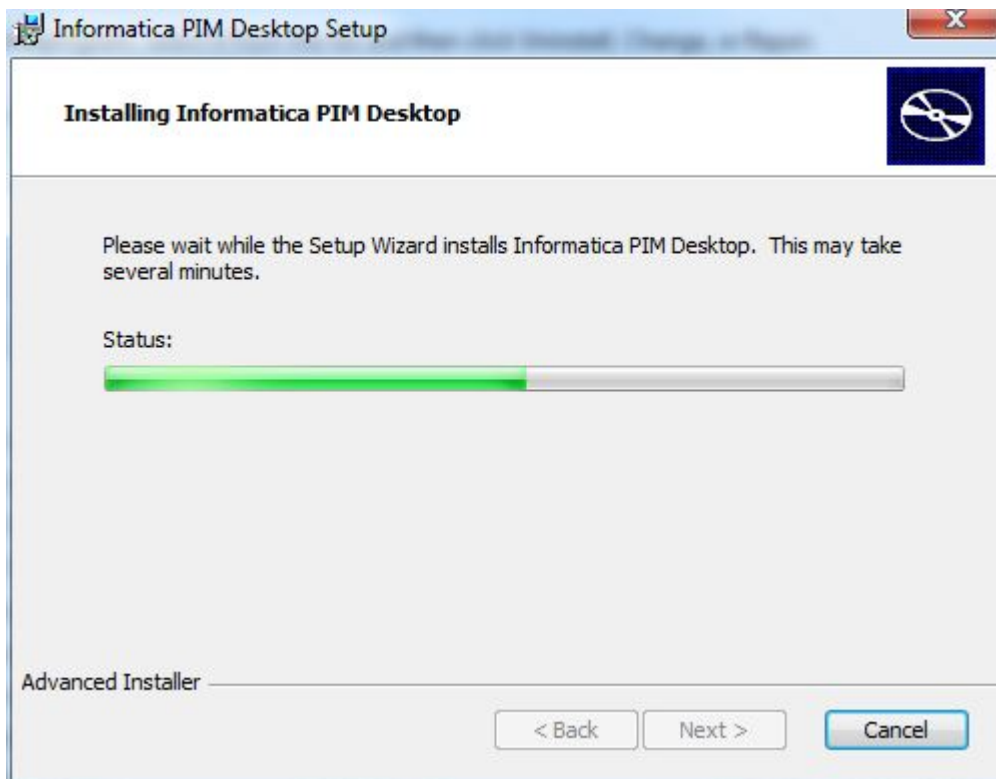
Selecting the installation folder

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.

i 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 than 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).



Server/Port:

OK

Cancel

Specify server settings

- 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.



Connection server:

OK

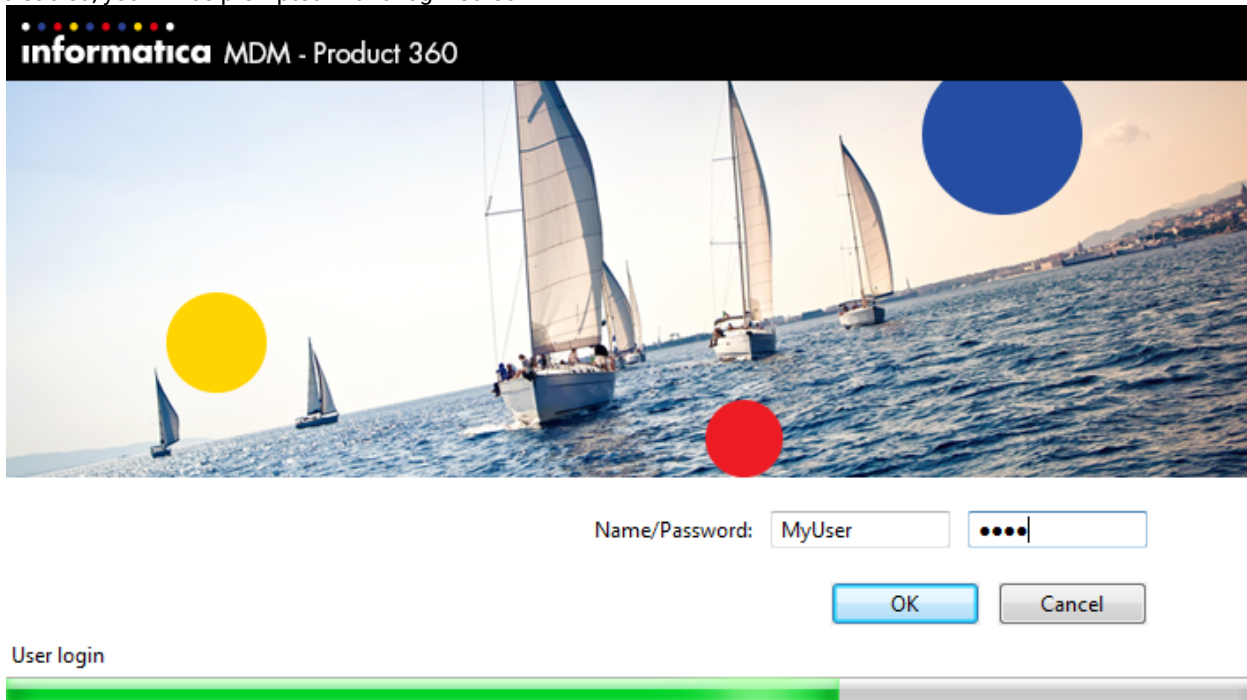
Cancel

Select server to connect

- 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

i 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 the following products, and has to be installed before them:

- Product 360 - AuditTrail
- Product 360 - Media Manager

Information for Message Queue configuration for Audit Trail

Product 360 - Audit Trail feature is using Apache ActiveMQ JMS server and one of its features called virtual topics. The idea of virtual topics is to create a message routing from JMS topic to JMS queue. The main difference between topic and queue is communication model: queue is point-to-point and topic is publish-subscriber. In other words it is possible once to read a message from a queue and it is possible to read same message multiple time from topic. You can read more about it here.

In Product 360 - Audit Trail the Informatica Product 360 - server is writing messages to a topic but Product 360 - Audit Trail server is reading topic from a queue. In order to route messages from topic to queue we rely on ActiveMQ virtual topics. No extra configuration in JMS server is required to setup that routing rather ActiveMQ uses a naming convention for topic and queues. Thus is it important to correctly configure topic and queue in Product 360 - server and Product 360 - Audit Trail server respectively. See notes in server.properties and audittrail.properties file and note blocks in the document.

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:**.
4. Launch the application using the script **C:\MessageQueue\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. Call **InstallService.bat** in directory **C:\MessageQueue\activemq\bin\win64**.
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 Active MQ 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="atcsreader" password="arpass"
        groups="atreaders,users"/>
      <authenticationUser username="atcswriter" password="awpass"
        groups="atwriters,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="admins" />
          <authorizationEntry queue="USERS.>" read="users" write="users" admin="users" />
          <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="admins" />
          <authorizationEntry topic="USERS.>" read="users" write="users" admin="users" />
          <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>
```

This snippet should be added in <broker> tag. Most of it is default configuration from example. These lines define users used by Product 360 - AuditTrail:

```
<authenticationUser username="atcsreader" password="arpass" groups="atreaders,users"/>
<authenticationUser username="atcswriter" password="awpass" groups="atwriters,users"/>
```

Passwords should be changed. Remember to change them in server.properties files also.
These lines grant those users needed access rights:

```
<authorizationEntry topic="VirtualTopic.ATCS.ALL" read="atreaders,atwriters" write="atwriters" admin="atwriters"/>
<authorizationEntry queue="Consumer.ATCS.VirtualTopic.ATCS.ALL" read="atreaders" admin="atreaders"/>
```

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 **failover** 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>

```

11 Media Manager Installation

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

These 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](#)

11.2 Pre-Installation Checklist

11.2.1 OS User Permissions

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

Port	Protocol	Product 360 Module
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
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

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
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

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](#)
- The next step is to install the database, refer to [Setup Product 360 - Media Manager Database](#)
- The next step is to install the client modules, refer to [Installing the client modules](#) (important: restart the computer after installation)
- Install the Funcd, refer to [Installing Funcd](#)
- [Installing the web front end](#)
- 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 360 version 8): Setting up the Session Manager

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

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.

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.

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 [...]Volume0/opastool/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 $CLIENTS"
FUNC_HOME=$BASEDIR
export FUNC_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 ${WORKDIR}/tools/mogrify ]; then
    echo "ERROR: Executable '${WORKDIR}/tools/mogrify' not found"
    exit 1
fi

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

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

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

# Start and stop functions
start() {
    echo "Starting '$BASEDIR/$PROG $OPTS' ..."
    cd $BASEDIR && ./$PROG $OPTS
    RETVAL=$?

    if [ $RETVAL -eq 0 ]; then
        echo " started"
    else
        echo " Failure"
    fi

    echo
    return $RETVAL
}

stop() {
    echo "Stopping '$PROG' ..."
    killall "$PROG"
    RETVAL=$?
    if [ $RETVAL -eq 0 ]; then
        echo " stopped"
    else
        echo " Failure"
    fi

    echo
    return $RETVAL
}

restart() {
    stop
    start
}

```

```

}

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 Engineering
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.

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 Functd.
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

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 Functd.

Under Windows

1. On **Volume0** on your file server, switch to the directory **opasdata/update/win/ocInt** (or MAIN_DVD\setup\HMM\update\win\ocInt).
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 Functd**.
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 System 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 .

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

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:jtds:sqlserver://localhost:1433/opasdb</DATABASE_URL>`
`<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 'ssl=request' to your url.

The url would look like

```
jdbc:jtds:sqlserver://localhost:1433/opasdb;ssl=request
```

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 'jtds-1.3.1.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 'jtds-1.3.1.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.

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

- | | |
|---|----------------------------------|
| 1 | \$ cd /opt |
| 2 | \$ unzip OpasGWebServerLinux.zip |
- Set attributes to make scripts executable

1	\$ chmod 777 /opt/OpasGWebServer/*.sh
2	\$ chmod 777 /opt/OpasGWebServer/Tomcat/bin/*
3	\$ chmod 777 /opt/OpasGWebServer/java/bin/*
 - Change owner of installed package to service user

1	\$ chown -R serviceuser /opt/OpasGWebServer
---	---
 - Configure database connection in **/opt/OpasGWebServer/Tomcat/webapps/opas/base.cfg** .
 <DATABASE_URL>**jdbc:oracle:thin:@dbservername:1521:oracle_instance**</DATABASE_URL>
 <DATABASE_DIALECT>org.hibernate.dialect.Oracle10gDialect</DATABASE_DIALECT>
 <DATABASE_USER>OPASUSER</DATABASE_USER>
 <DATABASE_PASSWORD>**Password**</DATABASE_PASSWORD>
 - 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

```

1 $ mkdir /mnt/FileserverOrIP
2 $ mkdir /mnt/FileserverOrIP/OpasVolumes
3 $ mount -t cifs -o username=remoteserviceuser //FileserverOrIP/OpasVolumes /mnt/
4 FileserverOrIP/OpasVolumes
5 $ 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

```

1 //FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/OpasVolumes cifs
  user=remoteserviceuser,uid=localserviceuser,gid=localservicegroup 0 0

```

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

```

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

```

or to

```

1 //FileserverOrIP/OpasVolumes /mnt/FileserverOrIP/OpasVolumes cifs
  user=remoteserviceuser,uid=localserviceuser,gid=localservicegroup,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:

```

1 $ mount /mnt/FileserverOrIP/OpasVolumes

```

Modify fstab without reboot.

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

```

1 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

```

1 $ yum install ImageMagick

```

2. Edit `colorme-Skript`

```

1 $ cd /opt/OpasGWebServer/Tomcat/webapps/opas/custom/profiles/layout/template/
2 $ rm colorme.sh
3 $ cp colorme.sh_disabled colorme.sh
4 $ chmod 777 colorme.sh

```

3. Create symbolic links to ImageMagick-commands

```

1 $ cd /opt/OpasGWebServer/Tomcat/webapps/opus/custom/profiles/layout/template/
2 imagemagick/
3 $ ln -s /usr/bin/composite composite
4 $ 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.

```

1 $ mkdir /mnt/FileserverOrIP
2 $ mkdir /mnt/FileserverOrIP/xobWorkdir
3 $ mount -t cifs -o username=serviceuser //FileserverOrIP/xobWorkdir/mnt/FileserverOrIP/
4 xobWorkdir
5 $ mkdir /FileserverOrIP
   $ ln -s /mnt/FileserverOrIP /FileserverOrIP

```

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:@dbservername: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 strong cryptographic algorithms to encrypt/decrypt secure information

Due to import control restrictions of some countries, the JCE policy that are bundled in the Java 8 Runtime Environment allow "strong" but limited cryptography is used by default. This means if you want to use a strong cryptographic algorithm like AES-256 you will need to change the configuration in file `<PIM ROOT>\server\jre\lib\security\java.security`. Enable the property `'crypto.policy=unlimited'` to activate the unlimited cryptographic algorithms. Otherwise you will run into errors during encryption/decryption in Product 360, saying you're using an illegal key size.

Also after update to newest Hotfix the Java JCE `'java.security'` file must be replaced in corresponding `jre\lib\security` folders of all Product 360 components.

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

11.3.7 Installation - General aspects

General requirements

Besides the appropriate Informatica Media Manager Process Engine package for your operating system, which can be Windows or Linux, two other tools have to be installed:

- ExifTool
- ImageMagick

ExifTool

You can obtain ExifTool from the following web page: <http://owl.phy.queensu.ca/~phil/exiftool/>

Installation for various systems is described on this web page: <http://owl.phy.queensu.ca/~phil/exiftool/install.html>

Depending on the operating system you're using it may also be available in the system's package manager.

ImageMagick

You can obtain ImageMagick and installation instructions from the following web page: <http://imagemagick.org/script/download.php>

Depending on the operating system you're using it may also be available in the system's package manager.

Installation - Linux

Prerequisites

As mentioned in [Installation - General aspects](#) you need the Linux package of Informatica Media Manager Process Engine. Also ExifTool and ImageMagick have to be installed on the system.

Installation steps

Perform the following steps to install Informatica Media Manager Process Engine on a Linux system.

1. Copy the MediaManagerProcessEngine-linux-[version].zip package to the folder /opt and go to that directory.

```
[... ~]$ cp [package] /opt  
[... ~]$ cd /opt
```

2. Unpack the archive and go to the extracted directory.

```
[... opt]$ unzip MediaManagerProcessEngine-linux-[version].zip  
[... opt]$ cd MediaManagerProcessEngine
```

3. Adjust the execution rights for the file configure.sh.

```
[... MMPEngine]$ chmod +x configure.sh
```

4. Adjust the execution rights for Informatica Media Manager Process Engine using the file configure.sh.

```
[... MMPEngine]$ ./configure.sh
```

5. Start Informatica Media Manager Process Engine using the file `startup.sh`.

```
[... MMPEngine]$ ./startup.sh
```

6. You can stop Informatica Media Manager Process Engine using the file `shutdown.sh`.

```
[... MMPEngine]$ ./shutdown.sh
```

Complete the installation by following the instructions in [Configuration](#).

Installation - Windows

Prerequisites

As mentioned in [Installation - General aspects](#) you need the Windows package of Informatica Media Manager Process Engine. Also ExifTool and ImageMagick have to be installed on the system.

Installation steps

Perform the following steps to install Informatica Media Manager Process Engine on a Windows system.

1. Copy the `MediaManagerProcessEngine-win-[version].zip` to a folder of your choice.
2. Extract the contents of `MediaManagerProcessEngine-win-[version].zip`.
3. Go to extracted directory `MediaManagerProcessEngine`.
4. To start Informatica Media Manager Process Engine you have two options:
 - a. Start it manually using the file `startup.bat`.
 - b. Install it as a service using the file `installService.bat` and start the service afterwards in the Task Manager.
5. To stop Informatica Media Manager Process Engine you have to do one of the following, depending on whether you started it manually or as a service:
 - a. If you have started it manually, bring its console window in front and press `Ctrl + C` on your keyboard.



Do not close the window.

Never stop Informatica Media Manager Process Engine by simply closing the console window. In this case it is possible that you interrupt running processes which can lead to inconsistencies in the database where the process status is persisted.

- b. If you have started it as a service stop it using the Task Manager.

Complete the installation by following the instructions in [Configuration](#).

11.3.8 Configuration

General

This document describes how you deploy the default application and how you configure it. After you've completed this Informatica Media Manager Process Engine is ready and will start generating previews as soon as jobs are pending.



Activiti resources

For more Activiti resources and nomenclature go to <https://www.activiti.org/>. This site describes concepts and usage of Activiti extensively.

Parameter configuration

The following chapters describe how to configure the necessary parameters to get the application working. Each of the settings explained below is stored in the file `[...] \MediaManagerProcessEngine \Tomcat \webapps \activiti-app \WEB-INF \classes \processEngine.properties`.

Encrypted passwords in configuration file

Product 360 Media Manager Process Engine supports the encryption of secure information like passwords in the configuration file `processEngine.properties`. 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 `processEngine.properties` gets encrypted after startup.

For example

```
db.password = [_to_encrypt_]Password[_to_encrypt_]
```

Usage of strong cryptographic algorithms to encrypt/decrypt secure information

Due to import control restrictions of some countries, the JCE policy that are bundled in the Java 8 Runtime Environment allow "strong" but limited cryptography is used by default. This means if you want to use a strong cryptographic algorithm like AES-256 you will need to change the configuration in file `<PIM_ROOT> \server \jre \lib \security \java.security`. Enable the property `'crypto.policy=unlimited'` to activate the unlimited cryptographic algorithms. Otherwise you will run into errors during encryption/decryption in Product 360, saying you're using an illegal key size.

Also after update to newest Hotfix the Java JCE `'java.security'` file must be replaced in corresponding `jre \lib \security` folders of all Product 360 components.

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

Product 360 Media Manager Process Engine 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.

Volume 0

Volume 0 is the designation for the standard file server share where assets are stored. Adapt the values of the setting `mediamanager.volume0` according to your system.

Configuring the file server share

```
# Path replacement for Media Manager volumes.
# Restart for changes required: No
# Restart for new volumes required: Yes
mediamanager.volume0 = /mnt/MediaManagerServer/Volumes/Volume0
# mediamanager.volume1 =
# mediamanager.volume2 =
```


The exact look of this may vary, depending on if your Informatica Media Manager Process Engine is running on the file server or somewhere else.

You can define an arbitrary number of additional volumes by adding further `mediamanager.volume[x]` settings.

Paths to tools

The paths to ImageMagick and ExifTool need to be configured. Adapt the values of the settings `imagemagick.path` and `exiftool.path` according to your system.

Configuring ImageMagick and ExifTool

```
# Path to ImageMagick
# Restart required: No
imagemagick.path = /usr/bin
# Path to ExifTool
# Restart required: No
exiftool.path = /usr/bin
```

Database connection

The database connection string, user and password need to be configured. Adapt the values of the settings `db.dialect`, `db.connection`, `db.user` and `db.password` according to your system.

Configuring the database connection

```
# DB dialect. Possible values are 'org.hibernate.dialect.Oracle11gR2Dialect', 'org.hibernate.dialect.Oracle12cDialect' ,
'org.hibernate.dialect.SQLServer2008Dialect', 'org.hibernate.dialect.SQLServer2012Dialect'
# Restart required: Yes
db.dialect = org.hibernate.dialect.Oracle11gR2Dialect
# DB connection string. JDBC style.
# Restart required: Yes
db.connection = jdbc:oracle:thin:@localhost:1521:opasdb
# DB user
# Restart required: Yes
db.user = OPASUSER
# DB password
# Restart required: Yes
db.password = OPASSPASS
```

Below are some examples for valid connection strings.

Microsoft SQL Server

```
jdbc:jtds:sqlserver://[host name]:1433/[database name]
```

Oracle

```
jdbc:oracle:thin:@[host name]:1521:[database name]
```

Oracle with a secure connection

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=[host name])(PORT=[port]))(CONNECT_DATA=(SERVICE_NAME=[database name])))
```



Oracle with a secure connection

For a secure connection with Oracle to work you need to import the server's certificate into the key store of the Java Runtime that was shipped with the Informatica Media Manager Process engine. It resides under [Informatica Media Manager Process Engine root directory]\java\jre\lib\security\cacerts.

The default user name for the database is OPASUSER and the default password is OPASSPASS.

More configuration options

All basic configuration is completed now, but you can configure more of the Informatica Media Manager Process Engine's behavior. This is described in [Operation](#).

11.3.9 Operation

Advanced configuration

The following chapters describe how you can control a number of parameters regarding the generated previews and data storage in general. Each of the settings explained in the subchapters below is stored in the file [...]

\MediaManagerProcessEngine\Tomcat\webapps\activiti-app\WEB-INF\classes\processEngine.properties.

Adjusting preview quality

Per default a JPEG quality of 85% is used when the previews are compressed. This is configurable by modifying the value of the setting preview.quality.

Setting the preview compression quality

```
# Preview quality in percent.  
# Default: 85  
# Restart required: No  
preview.quality = 85
```

Allowed values range from 1 to 100. The value has to be an integer.

Adjusting preview resolutions

The resolutions of the previews are configurable by modifying the values of the settings preview.pixelHigh, preview.pixelMiddle and preview.pixelLow.

Modifying the high resolution preview

```
# Preview max pixel for high previews  
# Default: 880  
# Restart required: No  
preview.pixelHigh = 880  
# Preview max pixel for middle previews
```

```
# Default: 150
# Restart required: No
preview.pixelMiddle = 150
# Preview max pixel for low previews
# Default: 25
# Restart required: No
preview.pixelLow = 25
```

The values have to be integers.



Middle and low preview resolution

You can overwrite the standard values by adding the variables `PixelMiddlePreview` and `PixelLowPreview`, though it is not recommended. Many parts of the Informatica Media Manager GUI are built around the default resolutions.

Disable XMP data storage

Per default found XMP data is stored in the database. This is configurable by modifying the value of the setting `metadata.storexmpdata`.

Disable XMP data storage

```
# Store embedded meta data (XMP, Exif, IPTC) in Media Manager database
# Default: true
# Restart required: No
metadata.storexmpdata = true
```

Allowed values are `false` and `true`.

Count of jobs that are fetched per cycle

The count of jobs that are fetched per cycle is configurable by modifying the value of the setting `processengine.maxjobcount`.

Job count

```
# Count of jobs fetched from the DB within 1 cycle
# Default: 2
# Restart required: No
processengine.maxjobcount = 2
```

The value has to be an integer.

Using own default images

For assets where no preview could be generated a default image is used instead. Those images reside in `[Media Manager Process Engine]\Tomcat\webapps\activiti-app\defaultpreviews`.

The default images adhere to the following naming schema: `[EXTENSION]_[#].jpg`

EXTENSION is the extension of a given file format, where # represents the size.

For example the default images for a `.wav` file would be named like this:

- `WAV_0.jpg`
- `WAV_1.jpg`
- `WAV_2.jpg`

0 represents the smallest image, 1 the medium sized and 2 the largest one.

To add own default images copy them to the mentioned folder. To overwrite the existing default previews replace the existing files.

Adding a standard preview for all unknown file formats is possible by adding files where the leading extension is omitted.

Logging

Logging is configured in the file [...]MediaManagerProcessEngine\Tomcat\webapps\activiti-app\WEB-INF\classes\log4j.properties.

There are four loggers provided by Informatica:

- `com.heiler.imm.connector`
 - Logging all the calls executed by Media Manager Connector
- `com.heiler.imm.internal`
 - Logging internal details (e.g. LDAP login)
- `com.informatica.imm.im4java`
 - Logging for ImageMagick calls and responses
- `com.informatica.imm.processengine`
 - Logging all process engine calls and responses
- `com.informatica.imm.processenginealive`
 - Logging each time a new cycle of the Media Manager Process Engine starts

Activiti has its own defined logger:

- `org.activiti.engine`

Logging levels for `com.informatica.imm.processengine`

There are four different logging levels available. The table below explains the four different logging levels ordered by increasing verbosity.

Logging level	Logged data
OFF	<ul style="list-style-type: none">• Nothing is logged
ERROR	<ul style="list-style-type: none">• All exception which are thrown are logged
DEBUG	<ul style="list-style-type: none">• Executed tasks including the duration of the execution• Fired calls against external tools including the file name
TRACE	<ul style="list-style-type: none">• Parameters of calls• Results of actions, including values, e.g. when <code>identify</code> has been called



Informatica Media Manager Connector

The Media Manager Connector loggers `com.heiler.imm.connector` and `com.heiler.imm.internal` support the logging level `DEBUG` only.

Example

The following is an example for the logging settings regarding the Informatica Media Manager Process Engine in `resources/log4j.properties`.



Please note that this file contains other logging settings as well.

Informatica Media Manager Process Engine login settings

```
# Basic setting
logs.basedirectory=/var/log/P360ProcessEngine
logs.conversionPattern=%d{ISO8601} [%t] %c{5}: - %m%n

# Direct log messages to a log file
log4j.appender.fileConnector=org.apache.log4j.RollingFileAppender
log4j.appender.fileConnector.File=${logs.basedirectory}/mediaManagerConnector.log
log4j.appender.fileConnector.MaxFileSize=5MB
log4j.appender.fileConnector.MaxBackupIndex=5
log4j.appender.fileConnector.layout=org.apache.log4j.PatternLayout
log4j.appender.fileConnector.layout.ConversionPattern=${logs.conversionPattern}

log4j.appender.fileConnectorHibernate=org.apache.log4j.RollingFileAppender
log4j.appender.fileConnectorHibernate.File=${logs.basedirectory}/mediaManagerConnectorHibernate.log
log4j.appender.fileConnectorHibernate.MaxFileSize=5MB
log4j.appender.fileConnectorHibernate.MaxBackupIndex=5
log4j.appender.fileConnectorHibernate.layout=org.apache.log4j.PatternLayout
log4j.appender.fileConnectorHibernate.layout.ConversionPattern=${logs.conversionPattern}

log4j.appender.fileProcessEngine=org.apache.log4j.RollingFileAppender
log4j.appender.fileProcessEngine.File=${logs.basedirectory}/processEngine.log
log4j.appender.fileProcessEngine.MaxFileSize=5MB
log4j.appender.fileProcessEngine.MaxBackupIndex=5
log4j.appender.fileProcessEngine.layout=org.apache.log4j.PatternLayout
log4j.appender.fileProcessEngine.layout.ConversionPattern=${logs.conversionPattern}

log4j.appender.fileIm4java=org.apache.log4j.RollingFileAppender
log4j.appender.fileIm4java.File=${logs.basedirectory}/im4java.log
log4j.appender.fileIm4java.MaxFileSize=5MB
log4j.appender.fileIm4java.MaxBackupIndex=5
log4j.appender.fileIm4java.layout=org.apache.log4j.PatternLayout
log4j.appender.fileIm4java.layout.ConversionPattern=${logs.conversionPattern}

log4j.appender.fileProcessEngineAlive=org.apache.log4j.RollingFileAppender
log4j.appender.fileProcessEngineAlive.File=${logs.basedirectory}/processEngineAlive.log
log4j.appender.fileProcessEngineAlive.MaxFileSize=1MB
log4j.appender.fileProcessEngineAlive.MaxBackupIndex=0
log4j.appender.fileProcessEngineAlive.layout=org.apache.log4j.PatternLayout
log4j.appender.fileProcessEngineAlive.layout.ConversionPattern=${logs.conversionPattern}

# Direct log messages to stdout
log4j.appender.stdout=org.apache.log4j.ConsoleAppender
log4j.appender.stdout.Target=System.out
log4j.appender.stdout.layout=org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern=${logs.conversionPattern}

# Root logger option
log4j.rootLogger=ERROR, stdout

# Log everything. Good for troubleshooting
log4j.logger.org.hibernate=OFF
```

```
# Log all JDBC parameters
log4j.logger.org.hibernate.SQL=OFF, fileConnectorHibernate

log4j.logger.com.heiler.imm.connector=ERROR, fileConnector
log4j.logger.com.heiler.imm.internal=OFF

log4j.logger.com.informatica.imm.processengine=INFO, fileProcessEngine
log4j.logger.com.informatica.imm.im4java=ERROR, fileIm4java
log4j.logger.com.informatica.imm.processenginealive=INFO, fileProcessEngineAlive

log4j.logger.org.activiti.engine.impl.bpmn.behavior.BpmnActivityBehavior = ERROR

# Custom tweaks
log4j.logger.com.codahale.metrics=WARN
log4j.logger.com.ryantenney=WARN
log4j.logger.com.zaxxer=WARN
log4j.logger.org.apache=WARN
log4j.logger.org.hibernate.engine.internal=WARN
log4j.logger.org.hibernate.validator=WARN
log4j.logger.org.springframework=WARN
log4j.logger.org.springframework.web=WARN
log4j.logger.org.springframework.security=WARN
```

11.4 Media Manager Integration

11.4.1 Product 360 - Server

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 version 8.0.5 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 . <div> If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.</div>
hmm.login.customer	Customer ID for the authentication at Product 360 - Media Manager.
hmm.db.url	Url of the Media Manager database which can be reached by Product 360. <div> 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 <div>jdbc:jtds:sqlserver://localhost:1433/opasdb;ssl=request</div></div>

Property	Description
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.connection.poolsize	Size of connections pool per Product 360 user to Media Manager, default value is 10.
hmm.connection.timeoutSEC	Time out setting(in seconds) for each connection to Media Manager. The connection will be deteled 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	Path to the share containing the temporary exported zip file for images. This share must provide read-write access to application server.
<div>  Removed since Product 360_8.0.03 </div>	

 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 functionality 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	<p>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".</p> <div>  Example hmm.jms.connection.url = failover:(tcp://JMSServer:61616?wireFormat.maxInactivityDuration=0)?initialReconnectDelay=2000&maxReconnectAttempts=2 </div>
hmm.jms.connection.username	<p>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.</p> <div>  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. </div>
hmm.jms.connection.password	<p>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.</p> <div>  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. </div>

Write access

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

Property	Description
hmm.supportsWrite	<p>Set this to false, If the write access of media manager Provider should not be supported. Please note, that there is not granular distinction. Either the Provider supports FULL write support (Upload, Removing files and categories...) or doesn't support write at all.</p> <div>  Default value true </div>

Property	Description
hmm.defaultCategoryId	<p>The identifier of default category(usually names "Unassigned") which stores all images that are not assigned to other categories.</p> <div>  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' </div>

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	<p>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.</p> <p>For more detailed information please visit the section "Media Asset Parallel Management" of chapter "Tuning advisory" in [OpertationManual].</p>	1000
hmm.numberOfThreads.initValue	<p>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.</p>	1

Property	Description	Default value
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.	original image
hmm.exportMediaAsset.defaultWithLoggedInUser	<p>Specifies whether the logged in user will be used as default while exporting media asset information from the Media Manager.</p> <p>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. Otherwise 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").</p>	true
hmm.exportMediaAsset.uncpath.separator	<p>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("/")</p>	\\

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)
<pre>##### ### connection settings for the application server ### ----- ### Connection data # # supervisor user in media manager with all rights</pre>

[illegible]

```

### 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 activated 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".

i 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.

The screenshot shows the repository editor interface. On the left, a tree view lists various field types under 'MediaAssetDocumentAttributesType', including 'NameHMM', 'AgencyIdHMM', 'LevelHMM', 'StateHMM', 'StatusHMM', 'FinishedHMM', 'InProgressHMM', 'ClassHMM', 'MemoHMM', and 'LicenseFreeHMM'. The 'LicenseFreeHMM' field type is selected. On the right, the configuration table for this field type is displayed:

Identifier	MediaAssetDocumentAttributesType.LicenseFreeHMM
Inactive	true
Object Name	licenseFreeHMM
Proxy Transition Entity Type	
Persistence	
Fragment Column Access	
Persistence Class Name	java.lang.String
Persistence Model Class	
Persistence XPath	F_IMGITEM.IMI_ITEM1
Physical Column Is Big	false

Below the configuration table, the 'custom' area shows a new field type being added under the entity 'MediaAssetDocumentAttributesType'. The field type is named 'License free' and has a field parameter 'mediaAssetProvider' with a value of 'HMM'.


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

i 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)

The screenshot shows the repository editor interface. On the left, a tree view lists various field types under 'MediaAssetDocumentAttributesType', including 'Class', 'Memo', 'License free', and 'Field Param mediaAssetProvider'. The 'Field Param mediaAssetProvider' field type is selected. On the right, the configuration table for this field type is displayed:

Property	Value
Documentation	
Name	mediaAssetProvider
Value	HMM

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 regular 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](#)
- [Supplier Portal Integration](#)
- [Media Manager and Supplier Portal Integration](#)
- [Web and Supplier Portal Integration](#)
- [Server Installation on Windows](#)
- [Server Installation on Linux](#)
- [Language Pack Installation](#)
- [Installation Troubleshooting](#)

12.1 Pre-Installation Checklist

12.1.1 OS User Permissions

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.

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 recommend 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:

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"
        URLEncoder="UTF-8" />

...

<Connector port="8090" 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

12.2.1 Prerequisite

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

- Server Installation
- [Desktop Client Installation](#)

12.2.2 Setup Product 360 Core Users and Permissions

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.

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:

Rights group	Permission	Note
Catalog	Supplier catalogs, general access	

Rights group	Permission	Note
General	Service Login	
Company Management	Company Management, general access	
Item	Items, general access	
Item	Create Item	
Item	Create Prices	
Item	Create Prices (in the past)	
Item	Delete items	
Item	Delete prices	
Item	Delete prices (in the past)	
Item	Edit items	
Item	Edit prices	
Item	Edit prices (in the past)	
Item	View prices	
Suppliers	Supplier Management, general access	
Suppliers	Edit suppliers	
Structures	Structures, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Structure groups	Structure groups, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Users	Users, general access	



All other Action rights not mentioned above, as well as all field rights have to be defined individually depending on the scenario and requirements of the project and the individual use case scenarios

Create Product 360 Supplier Portal System User

- 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 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**.

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 are 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 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 need at least the following action rights:

Rights group	Permission	Note
Web Permissions	Log in (Product 360 - Web)	
Web Permissions	Classify objects (Product 360 - Web)	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Web Permissions	Context visibility: Structures (Web Access)	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Catalog	Supplier catalogs, general access	
Structures	Structures, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Structure groups	Structure groups, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Item	Items, general access	
Item search	Item search management, general access	

Rights group	Permission	Note
Product	Products, read object rights	needed since version 7.1.02, while supplier is able to classify in structure tree.
Product	Product management, general access	needed since version 7.1.02, while supplier is able to classify in structure tree.
Variant	Variants, read object rights	Only in 3 tier product paradigm. Needed since version 7.1.02, while supplier is able to classify in structure tree.
Variant	Variant management, general access	Only in 3 tier product paradigm. Needed since version 7.1.02, while supplier is able to classify in structure tree.
Tasks	Task management, general access	Needed since version 8.1.0.00 for viewing supplier tasks
Tasks	Edit tasks	Needed since version 8.1.0.00 for working on supplier tasks

3. at least the following action rights have to be **revoked**:

Rights group	Permission	Note
Web Permissions	Tab visibility: Item, References (Product 360 - Web)	
Web Permissions	Classify objects (Product 360 - Web)	Needed since version 7.1.02, while supplier is able to classify in structure tree. So don't revoke while using version 7.1.02 and higher.
Web Permissions	Context visibility: Entire Context selection area (Product 360 - Web)	Needed since version 7.1.02, while supplier is able to classify in structure tree. So don't revoke while using version 7.1.02 and higher.
Web Permissions	Help (Product 360 - Web)	
Web Permissions	Change Password	
Tasks	Create tasks	
Multimedia attachments	Add multimedia attachments	
Import	revoke all permissions	Especially revoking 'Perform import' is important. Otherwise the Supplier Portal upload process would be compromised.

Rights group	Permission	Note
Merge	Merge, general access	Needed since version 8.1, since it allows to perform a catalog merge from within the Web UI now.
Merge	Perform Merge	Needed since version 8.1, since it allows to perform a catalog merge from within the Web UI now.
Flexible UI	Access Flexible UI	Needed since version 8.1 which introduces the new permission to avoid access to tasks of other suppliers and to objects from catalogs of other suppliers and master catalog using Flexible UI.

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 following field right setup should be considered:

Data range	Permission	Note
Tasks	Revoke all field rights except the following: Start date Estimated start date Anticipated completion on Progress Completed on	These adjustments are needed since version 8.1 which enables the assignment of Supplier Organizations to tasks. Revoking the field rights will guarantee that a supplier user cannot change the general definitions of a task setup by you.



All other Action rights not mentioned above, as well as all field rights have to be defined individually depending on the scenario and requirements of the project and the individual use case scenarios

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 need at least the following action rights:

Rights group	Permission	Note
Web Permissions	Log in (Product 360 - Web)	
Catalog	Supplier catalogs, general access	

Rights group	Permission	Note
Structures	Structures, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Structure groups	Structure groups, general access	Needed since version 7.1.02, while supplier is able to classify in structure tree.
Item	Items, general access	
Item search	Item search management, general access	
Product	Products, read object rights	needed since version 7.1.02, while supplier is able to classify in structure tree.
Variant	Variants, read object rights	Only in 3 tier product paradigm. Needed since version 7.1.02, while supplier is able to classify in structure tree.

3. at least the following action rights have to be **revoked**:

Rights group	Permission	Note
Web Permissions	Tab visibility: Item, References (Product 360 - Web)	
Web Permissions	Classify objects (Product 360 - Web)	
Web Permissions	Context visibility: Entire Context selection area (Product 360 - Web)	
Web Permissions	Help (Product 360 - Web)	
Web Permissions	Change Password	
Tasks	Create tasks	
Multimedia attachments	Add multimedia attachments	
Item	revoke all permission to edit, insert, delete or change items	
(Variants) only for 3 tier product paradigm installations	revoke all permission to edit, insert, delete or change variants	
Products	revoke all permission to edit, insert, delete or change products	

Rights group	Permission	Note
Import	revoke all permissions	Especially revoking 'Perform import' is important. Otherwise the Supplier Portal upload process would be compromised.



All other Action rights not mentioned above, as well as all field rights have to be defined individually depending on the scenario and requirements of the project and the individual use case scenarios

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**


12.2.3 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 <div style="border: 1px solid #f9c77d; padding: 10px; margin-top: 10px;">  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>
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

12.3.1 Prerequisite

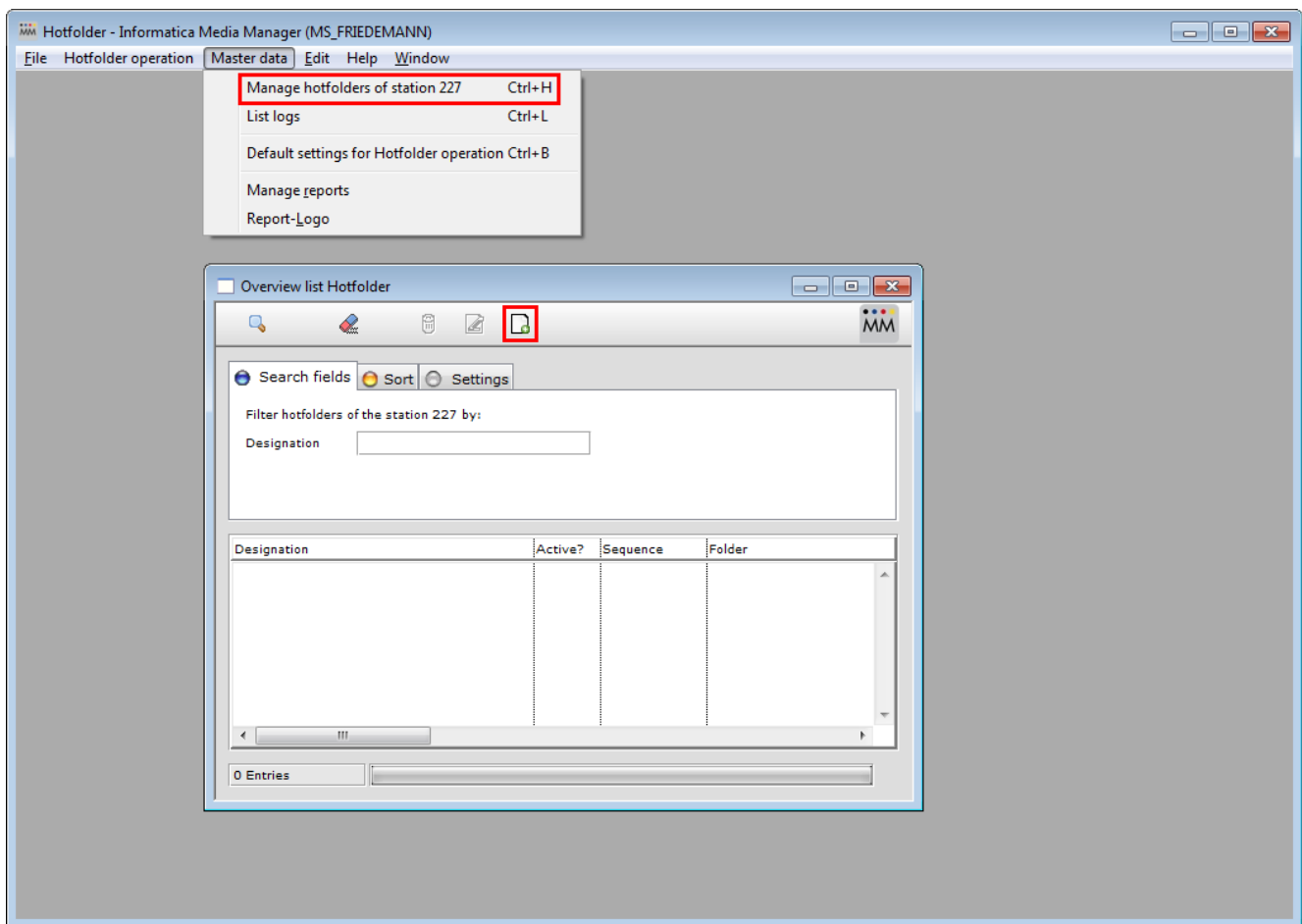
Before you can start with this chapter, you need to have finished the following parts:

- [Product 360 - Media Manager Installation](#)

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 definition.

Hotfolder modify the station 227

Entries of Hotfolder

Standard Output Upload settings

Monitoring

Designation: HSX_Hotfolder 1

Order no.: 0

☐ Should monitoring be enabled?

☐ Monitor change of size?

Folder to be monitored: \\hsis2100\Volumes\Buffervolume\hotfolder\314\in 2

Extension for valid files with a period, e.g. .PDF (blank = all):

Extension for invalid files with a period, e.g. .TMP (blank = none):

Process

Mode: Catalog import 3

Upload folder for catalog zip files: 4

Folder to which files with errors are to be moved (Blank = Delete files with errors):

Cancel Save

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

Hotfolder modify the station 227

Entries of Hotfolder

Standard Output Upload settings

Dest./output

Select, where the data should be filed:

☐ Provision in a directory

☒ Check into MEDIAS

☐ Check into job

How should the associated client no. or job no. be determined?

☐ Calculate from selection below

☐ Calculate from file name following the pattern below

☒ Calculate from selection and add folders

Select storage location

\\hsis2100\Volumes\Volume0\opasdata\d030001

Client: Sample company D030001

Options

Status to be assigned to the media

* Define no state *

Access level to be assigned the media object

Target directory for addition to the original location (if blank, normal addition to Medias area)

\\hsis2100\Volumes\Volume0\opasdata\d030001\catalogs

☒ Should sub-folders also be transferred?

IP address and port of message queue server

tcp://hsis920:61616

Name of queue

heiler.hmm.backend.event

Cancel Save

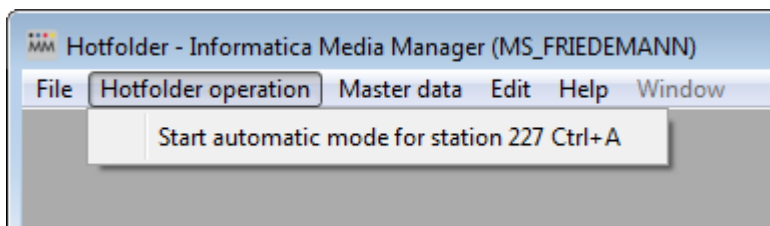
Additional settings are defined at the "Output" panel.

#1: Choose a customer. This customer has to be defined by 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.

Tomcat and Java

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

Installation HMM REST war

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

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=OPASSPASS
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:jtds:sqlserver://host:1433;DatabaseName=dbname
database.username=user
```

```
database.password=[_to_encrypt_]Password[_to_encrypt_]
database.driverClassName=net.sourceforge.jtds.jdbc.Driver
```



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.

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	
<code>web.client.hsx.supplier.login</code>	Product 360 Supplier Portal Item Editor System User e.g. <code>web.client.hsx.supplier.login=supplier</code>

web.client.hsx.supplier.password	Product 360 Supplier Portal Item Editor System User password <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>
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 <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>

12.5 Server Installation on Windows

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](#)
- [Product 360 Core and Supplier Portal Integration](#)
- [Product 360 - Media Manager and Supplier Portal Integration](#)
- [Product 360 - Web and Supplier Portal Integration](#)

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.



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 <div>  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. </div>
database.username	database user you created while setup the database. e.g. database.username=hsx
database.password	password for the above specified database user <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>

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 <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>

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. <code>hmm.restUri=http://hmmserver:8080/rest/rest</code>

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. <code>mail.enabled=true</code>
mail.protocol	Mail protocol as passed to javax.mail e.g. <code>mail.protocol=smtp</code>
mail.serverHost	Mail server host e.g. <code>mail.serverHost=smtp.company.com</code>
mail.serverPort	Mail server port e.g. <code>mail.serverPort=25</code>
mail.senderAddress Default	The default sender address for mails. Will be used and displayed as mail sender. e.g. <code>admin@company.com</code>
mail.username	User for mail server authentication. (only in case your mail server requires authentication)
mail.password	User password for mail server authentication. <div> If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.</div>

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/

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



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.

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.

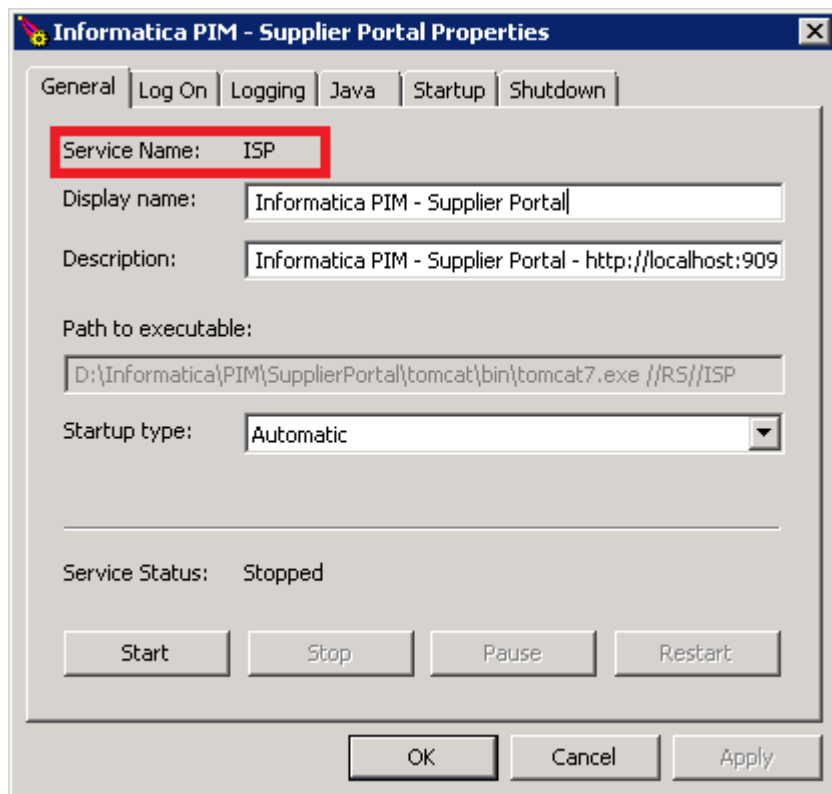
1. Open a new command line **with administrator privileges** (choose "Run as administrator" in context menu)
2. Navigate into the **<INSTALLATION ROOT>**
3. To install the tomcat with the default service name **Supplier Portal**, run the batch file **<INSTALLATION ROOT>/install.bat** to register the 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**

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.

(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.

Java

We do not distribute linux JDK or JRE with Supplier Portal. The JRE is already part of the Product 360 Core suite, or can be downloaded from the oracle website.

If you're not sure whether you have Java installed correctly:

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/jdk1.8.0`, 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.

If you need to install Java, follow these instructions:

1. Go to the Java download page and download the latest JRE or JDK.
2. When the download has finished, run the Java installer. Detailed installation instructions are provided on Oracle's website.

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.


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 <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;">  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. </div>
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. <code>hmm.restUri=http://hmmserver:8080/rest/rest</code>

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. <code>mail.enabled=true</code>
mail.protocol	Mail protocol as passed to javax.mail e.g. <code>mail.protocol=smtp</code>
mail.serverHost	Mail server host e.g. <code>mail.serverHost=smtp.company.com</code>
mail.serverPort	Mail server port e.g. <code>mail.serverPort=25</code>
mail.senderAddressDefault	The default sender address for mails. Will be used and displayed as mail sender. e.g. <code>admin@company.com</code>
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/

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 recommend 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>
```

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 service 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 Properties
# *****
# Java Application
# Locate the java binary on the system PATH:
#wrapper.java.command=../../jre/bin/java
# Specify a specific java binary:
#set.JAVA_HOME=/java/path
wrapper.java.command=/home/username/java/jdk1.8.0_45/bin/java
```

sudo

5. Install the server by executing the **<INSTALLATION ROOT>/pimsupplierportal.sh** script as root.

```
cd /opt/pim/supplierPortal
sudo ./pimsupplierportal.sh install
```

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
```

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 note that the language pack contains all language files, including German and English
 - Please make sure to backup the old content in case 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.	<ul style="list-style-type: none"> • 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.
Tomcat doesn't start.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
Tomcat starts but the webapp doesn't.	<ul style="list-style-type: none"> • 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 <i>RuntimeException</i> occurs which contains: <i>'Key length (256 bit) is greater than the max allowed key length (128 bit)'</i>.
The URL in the browser results in a 404 error message.	<ul style="list-style-type: none"> • 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
There's a spring error in the logs saying that table XYZ is missing.	<ul style="list-style-type: none"> • 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.

Problem	Possible solution
I changed a configuration property but it doesn't work.	<ul style="list-style-type: none"> 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.	<p>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</p> <p>see also in:</p> <ul style="list-style-type: none"> 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.	<p>Make sure that the following settings in the hsx.properties of the Product 360 server are set as follows:</p> <pre>hsx.enabled = true hsx.supliertasks.enabled = true</pre>
Tasks for suppliers (Task node "Tasks assigned to suppliers") are neither displayed in Desktop nor Web client.	<p>Make sure that the access right "Show tasks for all suppliers" is granted to the respective user group/organization.</p>

13 Audit Trail Installation

 This page describes the installation of the audit trail server and how to enable the audit trail feature in the Product 360 server

13.1 Prerequisite

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

- [Setup Product 360 - Audit Trail Database](#)
- [Product 360 Server Installation](#)
- [Desktop Client Installation](#)
- [Message Queue Installation](#)

13.2 Pre-Installation Checklist

13.2.1 OS User Permissions

Windows

- The users which install the Product 360 - Audit Trail modules need to be in the local Administrators group.

13.2.2 Audit Trail Default Ports

Port	Protocol	Product 360 Module	Description
61616	tcp	MessageQueue	This port is used for sending messages from Product 360 Core to Product 360 - Audit Trail server over MessageQueue.
2801	http	HTTP port	This port is used for the communication between Product 360 - Server and Product 360 - Audit Trail server (for obtaining change informations which are then displayed in the P360 - Desktop Client)

13.3 Audit Trail Server Installation

The Audit Trail binaries are part of the download package for Product 360.

13.3.1 Extract the Audit Trail archive

Choose your <ARCH> version and unpack the corresponding audit trail server archive PIM_<Version>_<Revision>_atserver<ARCH>.zip to an installation root <PIM_AUDITTRAIL_INSTALLATION_ROOT> (for example C:\INFORMATICA\PIM\AuditTrail).

Update configuration settings you can copy the properties you already configured while setup the database see [Audit Trail Database](#).


13.3.2 Configure the server connections

Following steps will configure the JMS consumer settings.

- Go to <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/audittrailserver/server.properties
- Configure the [MessageQueue](#) connection

JMS settings	
jms.connection.url	tcp://<host>:<port> It has to match the audittrail.properties configuration in Product 360 - Server. Default: tcp://localhost:61616
jms.queue.name	<queue name> JMS subscription queue name. The consumer is using VirtualTopic Queue, so queue name should match Consumer. *.VirtualTopic.* pattern. Default: Consumer.ATCS.VirtualTopic.ATCS.ALL
Optional	Only needed if MessageQueue security is enabled.

JMS settings	
jms.connection.username	JMS consumer username. It has to match the MessageQueue activemq.xml authenticationUser. Default: atcsreader
jms.connection.password	JMS consumer password. It has to match the MessageQueue activemq.xml authenticationUser. Default: arpass

 Note that JMS consumer is using VirtualTopic queue. It means that the queue name should match the following pattern Consumer.<consumerUniqueName>.VirtualTopic.<rest of the topic name> where consumerUniqueName is a name of the consumer and can be what ever you want and "rest of the topic name" is a topic name defined in the Product 360 Core audittrail.properties file.

3. Enable or disable the server authentication in the server.properties file.

Remote access	
server.authentication.enabled	Turn authentication on/off Default: true

Each entry must have a unique identifier. If authentication is of, you can leave username and password empty but do not delete them completely.

Adjust these two files for each Audit Trail Server


4. Optional: Only necessary if Audit Trail server security is activated

- a. run <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/setup_console.bat (a console with *osgi*> prompt pops up)
- b. update remote access username/password for default user using **userSetPassword** command in console.

13.3.3 Configure the network configuration

Go to <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/audittrailserver/AuditTrailNetworkConfig.xml

The AuditTrailNetworkConfig.xml file holds all the information of the used audit trail network. For each Audit Trail server define a separate entry as follow. For the server installation you only need the entry for the specific server you want to install. But it is recommended to create this file with all servers and to copy this file to each server installation.

 If you want to encrypt the password please refer to chapter Encryption of secure information in the [Server Installation](#) manual.

```
<network>
  <node host="audittrail-loadbalancer" port="2801" username="Administrator" password="Administrator" />
</network>
```

Element / Attribute	Description	Required	Default
network	Root element of the network configuration, contains one or more nodes	yes	
network /node	Represents an Audit Trail server node in the cluster	yes	
identifier	Unique identifier of the node within the network. See <i>-Dppm.nodeIdentifier</i> command line argument below!	yes	
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.	yes	
port	The port that is used for the http connection to the server. In case https is desired the port of the https element is used (see below).	yes in case http is used no in case https is used	
username	Username used for Basic Authentication.	yes	
password	Password used for Basic Authentication.	yes	
network /node/ https	Defines whether https should be used for connection. https is automatically used if element exists.	No. Only required if https is the desired protocol.	
port	The port that is used for https connection.	yes	
alias	The alias of the certificate that is to be used for secure connection. Refers to an entry in the defined Keystore (see keystore configuration below).	yes	
password	Keystore entry password for the entry with the specified alias.	yes	
protocol	Https protocol to be used for secure connection. Possible values are "SSL", "SSLv2", "SSLv3", "TLS", "TLSv1", "TLSv1.1" or "TLSv1.2".	no	TL Sv 1.2
network /node/ keystore	Keystore configuration used for https connections for each node.	yes in case https connection is used.	
file	Filepath to the keystore file.	yes	

password	Password used for general keystore access to the defined keystore file.	yes	
----------	---	-----	--

13.3.4 Start Audit Trail server

Windows

1. Open the file <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/conf/wrapper.conf and make sure that the property – **Daudittrail.nodeIdentifier** has the correct identifier. It has to be the identifier as declared in the AuditTrailNetworkConfig.xml file.
2. Run <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/console.bat or install as system service <AUDITTRAIL_INSTALLATION_ROOT>/bin/serviceInstall.bat
3. Check <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/*.log and <PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/.error.log if server does not start.

Linux

1. Open the file <PIM_AUDITTRAIL_INSTALLATION_ROOT>/bin/conf/wrapper.conf and make sure that the property – **Daudittrail.nodeIdentifier** has the correct identifier. It has to be the identifier as declared in the AuditTrailNetworkConfig.xml file.
2. Open the terminal and navigate to the root installation folder <PIM_AUDITTRAIL_INSTALLATION_ROOT>
3. Type in the command **bin/console.sh** to start the server or **bin/serviceInstall.sh** to install the service. The user requires the permission to install services.
4. Start service with **bin/serviceStart.sh**
5. Check <PIM_AUDITTRAIL_INSTALLATION_ROOT>/configuration/*.log and <PIM_AUDITTRAIL_INSTALLATION_ROOT>/logs/.error.log if server does not start.

13.4 Configure Audit Trail in the Product 360 Application

The Audit Trail feature is delivered as part of the Server and Desktop Client package. By default the Audit Trail functionality is disabled. To enable this feature you have to configure the following properties in <PIM_SERVER_INSTALLATION_ROOT>\configuration\HPM\audittrail.properties file:

13.4.1 Enable Audit Trail

General settings	
audittrail.enabled	Enable or disable Audit Trail functionality. If Audit Trail is disabled there will be no performance overhead.

13.4.2 Message Queue Connection Configuration

Product 360 Application Server sends all modifications to the Message Queue server. Therefore a valid connection URL and a topic name need to be specified. In case the Message Queue Server is configured to accept only authenticated connections also the corresponding user name and password need to be defined here.

Message Queue settings (JMS = Java Message Queue)	
audittrail.jmsconsumer.jms.topic	JMS topic where Audit Trail Change Sets will be sent to. Default: VirtualTopic.ATCS.ALL

Optionally	Only needed if MessageQueue security is enabled.
<code>audittrail.jmsconsumer.jms.connection.username</code>	User for authentication with the message queue
<code>audittrail.jmsconsumer.jms.connection.password</code>	Password for authentication with message queue



The topic name should start with `VirtualTopic` prefix because ActiveMQ maps such topics to queues internally by a convention. In the Audit Trail storage server configuration corresponding queues have to be named `Consumer.*.VirtualTopic.<rest of the topic name>` where part of the queue name marked by asterisk should be different for each consumer.

Example:

`audittrail.jmsconsumer.jms.topic` = `VirtualTopic.ATCS.ALL` (in `audittrail.properties` file)

`jms.queue.name` = `Consumer.ATCS.VirtualTopic.ATCS.ALL` (in the Audit Trail server's `server.properties` file)

<code>audittrail.jmsconsumer.jms.connection.url</code>	JMS connection URL. Default: <code>tcp://localhost:61616</code>
<code>audittrail.jmsconsumer.jms.persisted</code>	Default: <code>false</code>



If messages are not persisted then they will be lost if JMS server crashes or is restarted but JMS server can become a performance bottle neck if messages are persisted (SSD or raid can help). You can see if JMS server is a bottle neck in JMX bean `com.heiler.ppm/auditTrail/auditTrailJmsStatisticsWaitingThreadsCount` attribute. Ideally it should be 0. The JMS server is definitely a bottle neck if `WaitingThreadsCount` equals `SessionPoolSize` or `auditTrailProcessorStatisticsPoolSize`.

13.4.3 ATCS local storage configuration

If JMS server temporary is not accessible then audit trail processor attempts to save ATCS records locally. Saved messages are sent to JMS as soon as JMS server become accessible. One can configure different types of local storage:

ATCS storage configuration	
<code>audittrail.jmsconsumer.storage.type</code>	<p><storage type> (Default: <code>file</code>)</p> <p><i>file</i> - each message is serialized to file - recommended</p> <p><i>discard</i> - messages discarded (ATCS records will be lost)</p> <p><i>jdbm</i> - storage based on JDBM (fast but not stable on large volumes)</p> <p><i>memory</i> - stores messages in memory</p>

13.4.4 Further Configuration

ATCS configuration	
<code>audittrail.atcsbuilder.locale</code>	Locale for object labels and entity names (Audit Trail saves object labels only in one language). If not defined then HPM server locale is used. Default: en_US
<code>audittrail.fetch.data.before.delete</code>	Should be true if hard deletes should be logged with identifiers and labels. Disabling this feature will improve performance, however only entity type will be logged for hard delete operations.

13.4.5 Audit Trail network configuration

Copy the already created `AuditTrailNetworkConfiguration.xml` file from the Audit Trail server installation to the configuration folder of all P360 servers.

Https connection between P360 server and Audit Trail server

It is possible to use a https connection between both modules. The Audit Trail server side is setup with mentioned `AuditTrailNetworkConfiguration.xml`. The `AuditTrailNetworkConfiguration.xml` on the P360 server side does not require a keystore configuration. The keystore defined in P360 server's `NetworkConfig.xml` is used to encrypt the connection.

Multiple Audit Trail servers behind a load balancer

Multiple Audit Trail servers require a load balancer between the P360 server and the Audit Trail servers. Please be aware that the load balancer might use different ports. In this case the load balancer port has to be used in the P360 server's `AuditTrailNetworkConfiguration.xml`.

13.4.6 Start Product 360 Server

In case of successful Audit Trail startup you should see the following log messages:

- *Initialize audit trail*
- *audit trail is enabled*
- *registering default audit trail processor*
- *Initialize audit trail completed*

13.5 Activate Audit Trail for Entities in Repository

Audit Trail can be activated for any root entity in the repository. An activation/deactivation on sub entity level is not supported. The setting of the root entity will always be used, independent of the setting for the sub entities.

1. Open the repository editor,
2. Go to Custom section and select a root entity
3. Set `Supports Audit trail` flag to *true* in order to activate Audit Trail for this entity

Audit Trail can be activated and deactivated any time.

14 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](#)
- [BPM specific configuration within server.properties](#)
- [Failsafe handling of calls to Informatica BPM](#)

14.1 Informatica BPM Installation

14.1.1 Informatica BPM Installation

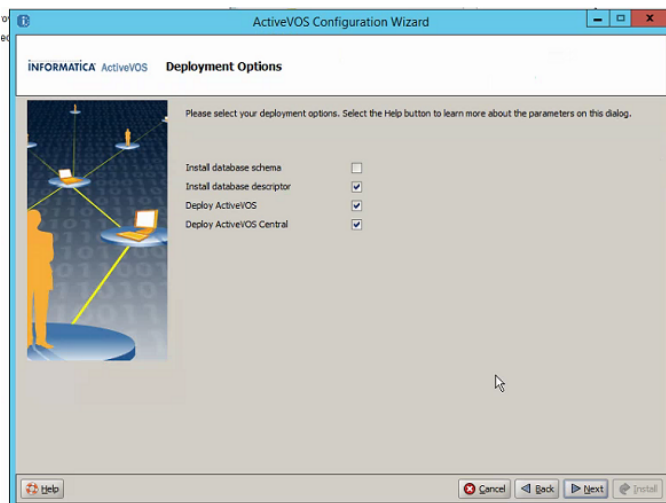
Installation of the Informatica BPM service

For the installation of the *Informatica BPM* service it is recommended to follow the official installation guide at http://infocenter.activevos.com/infocenter/ActiveVOS/v92/nav/3_0.

In the *Prerequisites* chapter http://infocenter.activevos.com/infocenter/ActiveVOS/v92/index.jsp?topic=%2Fdoc.server_install%2Ftomcat%2Fhtml%2FPrereqs.html&cp=3_0_1 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.



Webserver and Java

A good start is to use the integration with Apache Tomcat as container where *Informatica BPM* service will be deployed to.

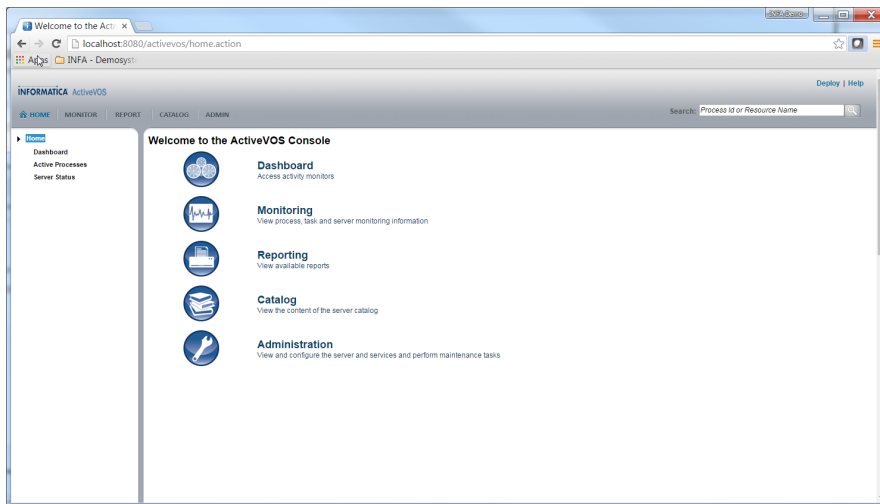


Make sure to use Java 7 as runtime for the *Informatica BPM* service by setting the necessary environment variables for example.

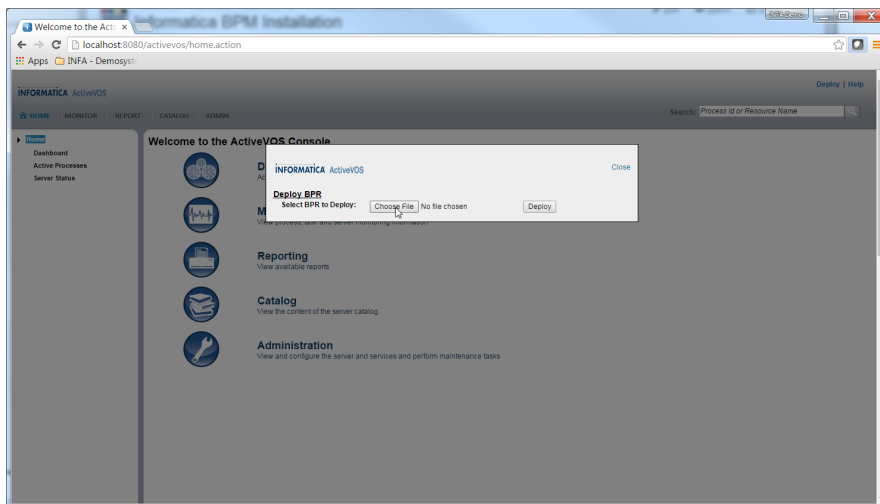
Post installation steps

After installing the *Informatica BPM* service a required default workflow has to be deployed to the BPM instance. This workflow is provided as deployable Business Process Archive *P360_BPM_Management.bpr* in the Accelerator package <P360 version>_InformaticaBPM of the P360 release.

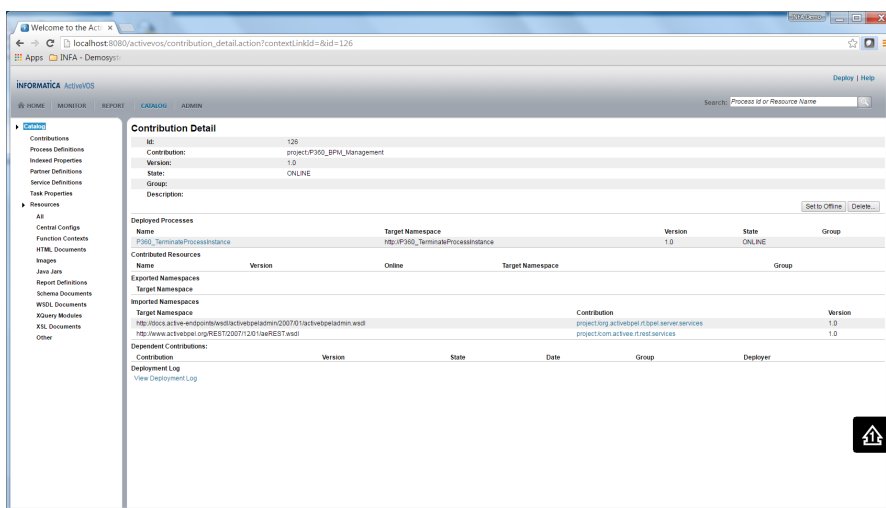
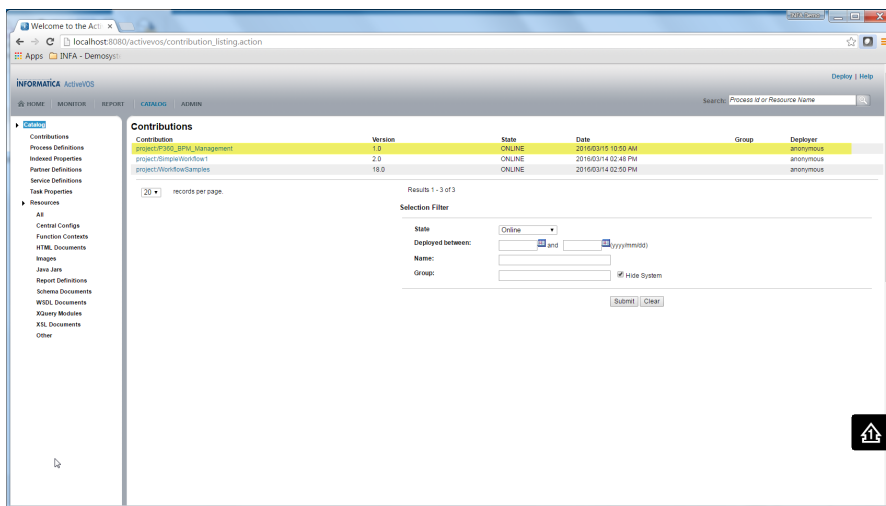
To deploy the workflow make sure the *Informatica BPM* service is up and running: Open your web browser and open the management console located at <http://your-bpm-server:8080/activevos>. You should see the start page of the management console.



To deploy the workflow open the deploy dialog by clicking on the "Deploy" button in the upper right corner and upload the Business Process Archive.



After the upload and deployment has been processed successfully you can check the availability of the P360 default workflow by navigating to *Catalog/Contributions* where you should now see the deployed project containing the P360 default workflow in the list.



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 (*sqljdbc.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\sqljdbc4.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

```
"<jdk7_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 (`sqljdbc4.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.

14.2 BPM specific configuration within server.properties

Once the "Informatica BPM" instance is up and running it's time to do the necessary configuration on P360 side. The configuration has to be done in the **<P360_SERVER_INSTALLATION_ROOT>\configuration\HPM\server.properties** file of the P360 server application.

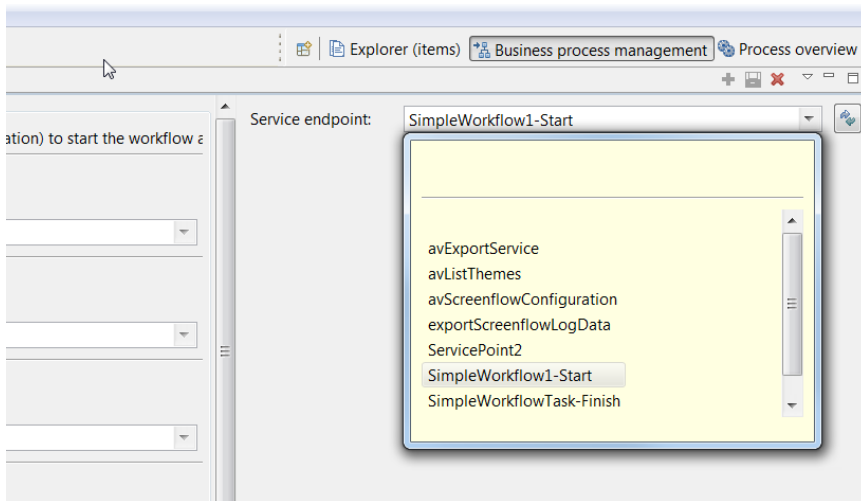
The following properties are relevant for configuration of the BPM integration.

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 <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>
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
infa.bpm.serviceendpoint.filter	No		Comma separated list, possibility of filtering out specific service endpoints, e.g.:serviceEndpoint1, serviceEndpoint2

 There are additional properties for enabling the fail-over handling, for details of these configuration properties please refer to [Failsafe handling of calls to Informatica BPM](#).

14.2.1 Simple connectivity test

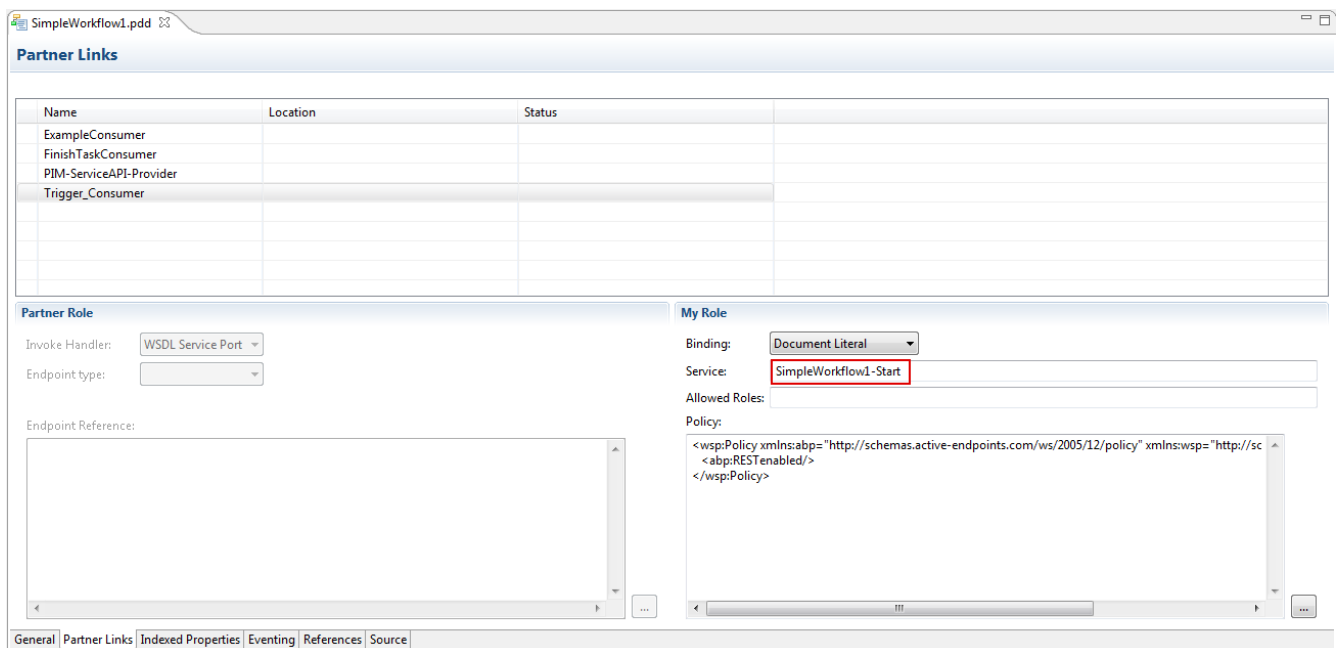
After installing the Informatica BPM service and configuration of the required properties on P360 side a first connectivity test can be done by opening the rich client with the "Business process management" perspective. In this perspective a new workflow trigger can be defined and available service endpoints can be assigned.



The drop-down list "Service endpoints" contains all service endpoints deployed to the Informatica BPM instance.

14.2.2 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.

Partner Links

Name	Location	Status
ExampleConsumer		
FinishTaskConsumer		
PIM-ServiceAPI-Provider		
Trigger_Consumer		

Partner Role

Invoke Handler:

Endpoint type:

Endpoint Reference:

```
<wsa:EndpointReference xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://schemas.xmlsoap.org/ws/2003/03/soap/address"
  <wsa:Address>http://<server-name>:<port>/wsa:Address
</wsa:EndpointReference>
```

My Role

Binding:

Service:

Allowed Roles:

Policy:

General | Partner Links | Indexed Properties | Eventing | References | Source

14.3 Failsafe handling of calls to Informatica BPM

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.throttlingDelayMilliseconds	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 <div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>
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

15 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](#)
- [Web Search Integration](#)
- [Server Installation on Windows](#)
- [Server Installation on Linux](#)
- [Installation Troubleshooting](#)
- Extended setup for high availability scenarios

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.

15.1 Pre-Installation Checklist

15.1.1 System Requirements

Memory Requirement

Product 360 - Web Search and the underlying Solr Server needs much RAM memory, that is completely allocated at start time ensuring a fast search index build and a web search:

- Minimum of 1.5 GByte is required
- 2 GByte is recommended

Java

An actual java **JDK8 64Bit** version is required for the use of Product 360 - Web Search.

It has to be ensured, that the system property **JAVA_HOME** is set to a JDK8 64Bit installation.

15.1.2 OS User Permissions

Windows

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

Linux

- The user which installs the Product 360 - Web Search needs to have administrative rights
- You need read/write permissions to the **<PIM_WEBSEARCH_INSTALLATION_ROOT>** directory.
- The user under which the service runs Product 360 - Web Search, also needs read/write permissions to the **<PIM_WEBSEARCH_INSTALLATION_ROOT>** directory.

15.1.3 Web Search Default Ports

Port	Protocol	Product 360 Module / Description
18090	http	Product 360 - Search Server (Tomcat Application Server)
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:

Change Application Server Ports

If you have another application running on your machine which is using the same ports that Product 360 Search uses by default, you may need to change the port which Product 360 Search will use.

You need to modify the server port (default is 18095), the http nio connector port (default is 18090) and the ajp connector port (default is 18100) to ports that are free on your machine.

1. Open file **<PIM_WEBSEARCH_INSTALLATION_ROOT>\configuration.properties**
2. Change Property:
 - `container.http.port`: http nio connector port (default is 18090)
 - `container.shutdown.port`: server port (default is 18095)
 - `container.ajp13connector.port`: ajp connector port (default is 18100)

This has to be done before running the Product 360 - Web Search installation.



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

15.2 Web Search Integration

15.2.1 Prerequisite

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

- Server Installation
- [Desktop Client Installation](#)
- Web Client Installation

15.2.2 Setup Product 360 Permissions for Web Search

There are 3 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 trigger or schedule the index updates.
3. **Technical Product 360 - Web Search REST User**
 - This technical user is used to authenticate REST requests at Product 360 - Server. All requests to fetch Product 360 data for a search index are run with this internal user.

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.

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	Search Index	Schedule Search Index access
2	Search Index	Search Index, general access

Please ensure to have all permission to entities, fields and attributes that are defined in the index configuration.

Permission Settings for Technical Product 360 - Web Search REST User

As a recommendation the **Technical Product 360 - Web Search REST User** need at least all read access of all catalogs, assortments, entities, fields and attributes that are defined in the index configuration.


Additionally the following permission has to be set:

No.	Rights group	Permission
1	General	Service Login
2	Catalog	Supplier catalogs, general access

15.2.3 Setup Configuration for Product 360 - Core

The configuration properties for Web Search on Product 360 Core can be defined in the property file **fulltextsearch.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	fulltextsearch.rest.url	http://localhost:18090/hps-web/rest2	URL path to the Web Search REST server.	Depending where the Web Search server is located, the server name (e.g. localhost) can be different. Depending on the Web Search configuration of <PIM_WEBSEARCH_INSTALLATION_ROOT>\configuration.properties the port can be different.
2	fulltextsearch.rest.username	config	Login name of the Web Search REST server.	To change the credential for the REST Services see: REST Credential Configuration
3	fulltextsearch.rest.password	Heiler33!	Login password of the Web Search REST server.	To change the credential for the REST Services see: REST Credential Configuration <div> If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.</div>
4	fulltextsearch.rest.allow.self-signed.certificate	false	Allows self-signed certificate for test purposes only if you use https. It is classified as unsafe.	



Tip

Please check your credential using the REST Url in your browser: <http://localhost:18090/hps-web/rest2/index/Master/Configuration/Online>

15.2.4 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**.

See also: Product 360 - Web Configuration#Product 360 - Web Search Integration (since version 7.0.03)

No.	Property	Default Value	Description
1	web.client.hps.max.display.facet	5	Maximum number of displayed search facets.







15.3 Server Installation on Windows

15.3.1 Create Your MDM P360 - Web Search Server Installation Root

Unzip the file MDM_P360_WebSearch_<Version>.zip from your installation package into an empty directory. In this manual we assume you are using the following installation root:

<WEBSEARCH_INSTALLATION_ROOT> = C:\INFORMATICA\MDM_P360_WebSearch

Screenshot: Product 360 - Web Search Folder Structure

	apache-tomcat-7.0.14	File folder
	internal	File folder
	solr	File folder
	configuration.properties	PROPERTIES File
	configure	Windows Command Script
	Readme	Text Document

15.3.2 Setup Web Search Configuration

The configuration properties for Product 360 - Web Search can be defined in the property file **configuration.properties**, located in **<PIM_SERVER_INSTALLATION_ROOT>**.

The Product 360 - Web Search Server has to be restarted in order to have changes take effect.


The configuration file itself contains properties following the standard "key: value" pattern.





Password

Passwords which contain backslashes "\" are not supported and can not be taken.

N o.	Property	Default Value	Description	Remarks
1	jdk.home	D:/java/jdk8 or C:/Program Files/java/jdk	Location of the java installation	

	Settings for customized EncryptionService			
2	ppm.encryptonService	< empty >	Full classname of a customized EncryptionService implementation (optional)	
3	ppm.encryptonService.configPath	< empty >	Location of properties files for customized EncryptionService implementation (optional)	
	WebSearch REST server settings			
4	fulltextsearch.rest.url	http://localhost:18090/hps-web/rest2	Base Url for REST.	
5	fulltextsearch.rest.username	config	Username of the REST user of WebSearch server	
6	fulltextsearch.rest.password	Heiler33!	Password of the REST user of WebSearch server	<div>  If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual. </div>
	HPM REST server settings			
7	hpm.rest.url	http://localhost:1512/rest	Base Url for REST.	
8	hpm.rest.username	rest	Username of the REST Product 360 user which has Service API access permissions.	

9	hpm.rest.password	heiler	Password of the REST Product 360 user	 If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
Settings for tomcat container				
10	container.http.port	18090	Tomcat http nio connector port	
11	container.shutdown.port	18095	Tomcat server port	
12	container.ajp13connector.port	18100	Tomcat ajp connector port	
13	container.admin.username	tomcat	Name of tomcat user	
14	container.admin.password	heiler	Password of tomcat user	 The password can be hashed. Please refer to chapter Web Container Password Hashing for further information.
15	container.log.dir	<PIM_WEBSEARCH_INSTALLATION_ROOT>/log	Location of the log file of the Web Search server	Web Search uses log4j for logging. The log4j.xml file is created running configure.cmd (see below). The log4j.xml file is located after that in <PIM_WEBSEARCH_INSTALLATION_ROOT>\apache-tomcat-7.0.14\lib.
16	container.service.name	MDM P360 Web Search 8.0.0	Name of the Web Search server	The name of the Windows Service is: <i>Informatica MDM P360 Web Search 8.0.0</i>
17	container.memory.max	1536	Maximum Memory which is provided for the Web Search server.	<p>As a minimum of 1.5 GByte is recommended.</p> <p>The Web Search server allocate all of the provided memory to improve performance during the search index build and the fulltext search procedure.</p>

18	password.hash.algorithm	SHA-512	Hash algorithm for password hashing in tomcats container. If this value is empty, a default value will be used: SHA-512. Possible values are: SHA-224, SHA-256, SHA-384, SHA-512.	For details see the MessageDigest section in https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#MessageDigest Java Cryptography Architecture Standard Algorithm Name Documentation for information about standard algorithm names.
Solr settings				
19	solr.home	\${hps.server.home}/solr/configuration	Location of the Solr configuration.	It is recommended not to change the solr configuration with the current Product 360 version.
20	search.solr.useHttps	false	http=false, https=true	If the solr server should run with https, this property should be set to true.
21	search.solr.host	localhost	Location of the Solr server.	
22	search.solr.port	18090	Port of the Solr server.	
23	solr.default.core.size	100000	This defines the maximum number of documents that will be indexed per solr core.	This is an important property for high volume installations. According to this property multiple solr cores will be created to keep the size of a single core small. The search on multiple cores will be performed with the solr distributed search.
24	solr.cluster.node.list		Definition of a comma separated list of solr nodes used for indexing multiple cores in round robin approach. The list has to be in the format server1:18090,server2:18090,server3:18090	This is an important property for high volume installations in combination with the property <i>solr.default.core.size</i> to spread multiple solr cores over different server nodes.



Please set the JAVA_HOME environment variable to any Java installation (this is used by the ant script, not the running Product 360 - Web Search)

15.3.3 Web Container Password Hashing

In servlet container like Tomcat password hashing is provided by default instead of password encryption. Therefore password hashing will be used to save tomcat container.

Product 360 Web Search Server supports password hashing of Web container passwords like of the tomcat admin user or the solr user.

In Version 8.0.6 only **Index Config Administration Tool** supports any authentication where credentials can be used. The currently used solr version 3.6 does not support any authentication.

The password hashing will be executed only if your secure information in the configuration files is enclosed by the marker `[_to_hash_]`. The hash algorithm is *SHA-512* and can be set with property: `password.hash.algorithm`. So, if you want to have e.g. the password "MyPassword" be hashed in the *configuration.properties* file, just use the marker before and after the password like this: `[_to_hash_]MyPassword[_to_hash_]`.

For example:

properties file

```
# container credentials
container.admin.user.name      = tomcat
container.admin.user.password = [_to_hash_]heiler[_to_hash_]
```

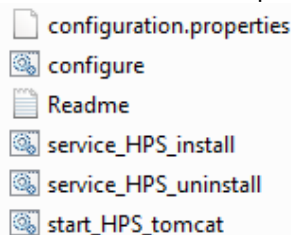
Disable Tomcats password authentication

If you don't want to use password authentication in tomcat container or you want to disable the Tomcat password hashing, following steps are needed to switch it off:

- Modify file: `web.xml` in folder: `<WebSearchInstallationRoot>\<tomcat-server>\webapps\hps-config-admin\WEB-INF` and comment the xml tags: `security-constraint`, `security-role` and `login-config`.
- Restart tomcat server

15.3.4 Create Web Search Server Start Script and Web Search Windows Service Script

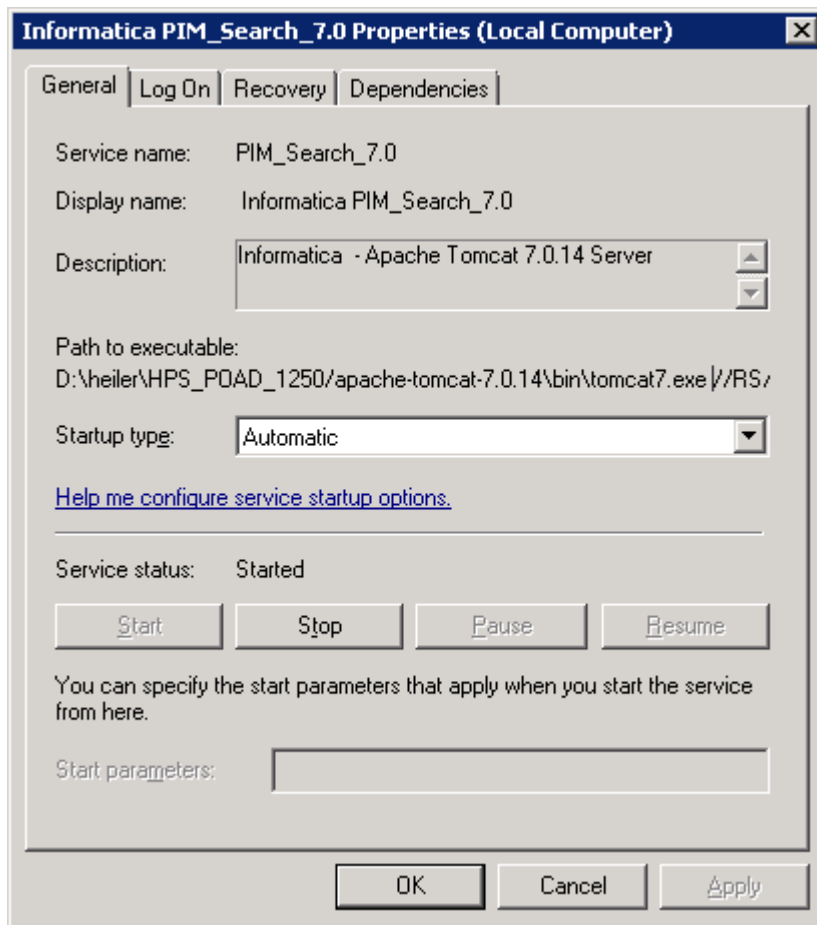
1. Run the `configure.cmd` script as **administrator**
2. Now the console start script file appears:



15.3.5 Start Web Search Server

There are two possibilities to start the Web Search server:

- Start Web Search server within a console, run `start_HPS_tomcat.cmd` script.
- Install Web Search server as a Windows Service, run `service_HPS_install.cmd` script as administrator user. After that start the Window Service **Informatica MDM P360 Search 8.0**.



15.3.6 Stop Web Search Server

There are two possibilities to stop the Web Search server as well.

- Use `Strg-c` to stop the Web Search Server that runs within a console.
- Stop the Window Service **Informatica MDM P360 Search 8.0**.

To remove the Web Search Windows Service run `service_HPS_uninstall.cmd` as administrator user.

15.4 Server Installation on Linux

15.4.1 Prerequisite



You will need root privileges to install the web search on your system.

15.4.2 Installation

Java

We do not distribute linux JDK or JRE with the Product 360 Web Search.

The JRE is already part of the Product 360 Core suite, or can be downloaded from the oracle website.

If you're not sure whether you have Java installed correctly:

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/jdk1.8.0`, 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 a service user without an linked shell you need to set the `JAVA_HOME` within the supplier portals wrapper.conf.

If you need to install Java, follow these instructions:

1. Go to the Java download page and download the latest JRE or JDK.
2. When the download has finished, run the Java installer. Detailed installation instructions are provided on Oracle's website.

Create the Product 360 - Web Search Server Installation Root



We recommend to create a service user to run the Product 360 search under a 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>
```

1. Unzip the file `MDM_P360_WebSearch_<Version>.zip` from your installation package into an empty directory

```
cd /opt/pim
sudo unzip MDM_P360_WebSearch_<Version>.zip
```


2. In this manual we assume you are using the following installation root:
<INSTALLATION ROOT> = /opt/pim/MDM_P360_WebSearch
feel free to change this to another location.
3. Change file and directory permissions



```
sudo chmod -R 755 /opt/pim/MDM_P360_WebSearch
```

15.4.3 Configuration

The configuration properties for MDM P360 - Web Search can be defined in the property file **<INSTALLATION ROOT>/configuration.properties**.

The configuration file itself contains properties following the standard "key: value" pattern.

Property	Default Value	Description	Remarks
jdk.home	/opt/java/jdk1.8.0	Location of the java installation	
Settings for customized EncryptionService			
ppm.encrypti onService	< empty >	Full classname of a customized EncryptionService implementation (optional)	
WebSearch REST server settings			
fulltextsearch .rest.url	http:// localhost: 18090/hps- web/rest2	Base Url for REST.	
fulltextsearch .rest.usernam e	config	Username of the REST user of WebSearch server	
fulltextsearch .rest.passwor d	Heiler33!	Password of the REST user of WebSearch server	 If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
HPM REST server settings			
hpm.rest.url	http:// localhost: 1512/rest	Base Url for REST.	
hpm.rest.user name	rest	Username of the REST Product 360 user which has Service API access permissions.	

hpm.rest.password	heiler	Password of the REST Product 360 user	 If you want to encrypt the password please refer to chapter Encryption of secure information in the Server Installation manual.
Settings for tomcat container			
container.http.port	18090	Tomcat http nio connector port	
container.shutdown.port	18095	Tomcat server port	
container.ajp13connector.port	18100	Tomcat ajp connector port	
container.admin.user.name	tomcat	Name of tomcat user	
container.admin.user.password	heiler	Password of tomcat user	 The password will be hashed. Please refer to chapter Web Container Password Hashing for further information.
container.log.dir	\${container.home}/../log	Location of the log file of the Web Search server	Web Search uses log4j for logging. The log4j.xml file is created running configure.cmd (see below). The log4j.xml file is located after that in <PIM_WEBSEARCH_INSTALLATION_ROOT>\apache-tomcat-7.0.14\lib.
container.service.name	MDM P360 Web Search 8.0.0	Name of the Web Search server	The name of the Windows Service is: <i>Informatica MDM P360 Web Search 8.0.0</i>
container.memory.max	1536	Maximum Memory which is provided for the Web Search server.	As a minimum of 1.5 GByte is recommended. The Web Search server allocate all of the provided memory to improve performance during the search index build and the fulltext search procedure.

password.hash.algorithm	SHA-512	Hash algorithm for password hashing in tomcats container. If this value is empty, a default value will be used: SHA-512. Possible values are: SHA-224, SHA-256, SHA-384, SHA-512.	For details see the MessageDigest section in https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#MessageDigest Java Cryptography Architecture Standard Algorithm Name Documentation for information about standard algorithm names.
Solr settings			
solr.home	\${hps.server.home}/solr/configuration	Location of the Solr configuration.	It is recommended not to change the solr configuration with the current Product 360 version.
search.solr.useHttps	false	http=false, https=true	If the solr server should run with https, this property should be set to true.
search.solr.host	localhost	Location of the Solr server.	
search.solr.port	\${container.http.port}	Port of the Solr server.	
solr.default.core.size	100000	This defines the maximum number of documents that will be indexed per solr core.	This is an important property for high volume installations. According to this property multiple solr cores will be created to keep the size of a single core small. The search on multiple cores will be performed with the solr distributed search.
solr.cluster.node.list		Definition of a comma separated list of solr nodes used for indexing multiple cores in round robin approach. The list has to be in the format server1:18090,server2:18090,server3:18090	This is an important property for high volume installations in combination with the property <i>solr.default.core.size</i> to spread multiple solr cores over different server nodes.



Please set the JAVA_HOME environment variable to any Java installation (this is used by the ant script, not the running of Product 360 - Web Search)

Web Container Password Hashing

In servlet container like Tomcat password hashing is provided by default instead of password encryption. Therefore password hashing will be used to save tomcat container.

Product 360 Web Search Server supports password hashing of Web container passwords like of the tomcat admin user or the solr user. The password hashing will be executed only if your secure information in the configuration files is enclosed by the marker `[_to_hash_]`. The hash algorithm is *SHA-512* and can be set with property: `password.hash.algorithm`. So, if you want to have e.g. the password "MyPassword" be hashed in the *configuration.properties* file, just use the marker before and after the password like this: `[_to_hash_]MyPassword[_to_hash_]`.

For example:

properties file

```
# container credentials
container.admin.user.name      = tomcat
container.admin.user.password = [_to_hash_]heiler[_to_hash_]
```

Disable Tomcats password authentication

If you don't want to use password authentication in tomcat container or you want to disable the Tomcat password hashing, following steps are needed to switch it off:

- Modify file: `web.xml` in folder: `<WebSearchInstallationRoot>\<tomcat-server>\webapps\hps-config-admin\WEB-INF` and comment the xml tags: `security-constraint`, `security-role` and `login-config`.
- Restart tomcat server

Generate install/remove/start/stop script

1. For security reasons, `sudo` may clear environment variables which is why it is probably not picking up `$JAVA_HOME`. Look in your `/etc/sudoers` file for `env_reset`. If it is set you need to add the following line to `/etc/sudoers` to keep `JAVA_HOME`.

```
Defaults    env_keep += "JAVA_HOME"
```

2. Run the `<INSTALLATION ROOT>/configure.sh` to generate the `<INSTALLATION ROOT>/pimsearch.sh` management script.

```
cd /opt/pim/MDM_P360_WebSearch
sudo ./configure.sh
```

3. Change ownership of `<INSTALLATION ROOT>` to **pim** user and group

```
sudo chown -R pim:pim /opt/pim/MDM_P360_WebSearch
```

15.4.4 Install Tomcat

A pre-configured Apache Tomcat is part of the Product 360 Web Search archive and can be found in the directory `<INSTALLATION ROOT>/apache-tomcat-<Version>`. It is recommended to run Product 360 Web Search Tomcat as an service.

Install Product 360 Web Search Tomcat Linux Service

1. (Optional) In case your service user is a system user with no linked shell you have to set the JAVA_HOME variable directly within Product 360 Web Search configuration wrapper.conf.
 - a. Go to the tomcat configuration directory and edit the wrapper configuration file **<INSTALLATION ROOT>/apache-tomcat-<Version>/conf/wrapper.conf**.

```
#*****
# Wrapper Java Properties
#*****
# Java Application
# Locate the java binary on the system PATH:
#wrapper.java.command=../../jre/bin/java
# Specify a specific java binary:
#set JAVA_HOME=/java/path
#wrapper.java.command=/home/username/java/jdk1.8.0_45/bin/java
```

sudo

2. To install the server execute the **<INSTALLATION ROOT>/pimsearch.sh** script as root.

```
cd /opt/pim/MDM_P360_WebSearch
sudo ./pimsearch.sh install
```

Start/Stop Product 360 Web Search Tomcat Server./pim

You can use the **<INSTALLATION ROOT>/pimsupplierportal.sh** script to start/stop the tomcat server with the Web Search using the service user account.

```
su pim
cd /opt/pim/MDM_P360_WebSearch

# to start the MDM-P360 Web Search
./pimsearch.sh start

# to stop the MDM-P360 Web Search
./pimsearch.sh stop

# get current service status
./pimsearch.sh status
```

Deinstallation

```
cd /opt/pim/MDM_P360_WebSearch
sudo ./pimsearch.sh remove
```

15.5 Installation Troubleshooting

In case the application doesn't work, you might try the following:

Problem	Possible solution
Installation by running the <code>configure.cmd</code> or <code>configure.sh</code> throws an <code>java.lang.UnsupportedClassVersionError</code> exception.	<p>May be a wrong java version is used. A JDK 8 64Bit java is necessary to install and run Web Search. Ensure that the <code>JAVA_HOME</code> system property shows to a JDK 8 64Bit installation path.</p> <p>Check that with <code>echo %JAVA_HOME%</code>.</p>
The Tomcat service registration fails with an error.	<ul style="list-style-type: none"> • 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.
<p>The Tomcat service registration fails with a java error:</p> <ul style="list-style-type: none"> • The <code>JAVA_HOME</code> environment variable is not defined correctly • <code>startup.bat</code> Files\Java\jdk1.8.0_111 was unexpected at this time. 	<p>Please check the <code>jdk.home</code> settings in the <code>configuration.properties</code> file.</p> <p>Ensure not to use spaces around the equal sign and use slashes instead of backslashes.</p> <p>Example: <code>jdk.home=C:/Program Files/Java/jdk8</code></p>
Tomcat doesn't start.	<ul style="list-style-type: none"> • Take a look at the Tomcat log files in <PIM_WEBSEARCH_INSTALLATION_ROOT>/apache-tomcat-7.0.42/logs • Make sure that the configured ports are not in use. You can change the ports in <PIM_WEBSEARCH_INSTALLATION_ROOT>/configuration.properties. And you have to repeat the Web Search installation. • 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 in <PIM_WEBSEARCH_INSTALLATION_ROOT>/configuration.properties. Make sure that you use a 64 bit Java version.
Tomcat starts but the webapp doesn't.	<ul style="list-style-type: none"> • Take a look at the Product 360 - Web Search log files in <PIM_WEBSEARCH_INSTALLATION_ROOT>/log or at Tomcat log files in <PIM_WEBSEARCH_INSTALLATION_ROOT>/apache-tomcat-7.0.42/logs • Make sure that the configuration.properties file and its properties are valid.

Problem	Possible solution
<p>Building search index failed on <code>http://server:port/hps-config-admin</code></p> <p>or on Product 360 Desktop in the Process Overview Perspective in the Index Search View.</p>	<ul style="list-style-type: none"> • Literal errors: The index configuration is not error tolerant. You have to use the exactly field- and identifier definition from hpm. Please have a look to the index example how it should looks like. • Not implemented yet: As mentioned above not all possible index configuration settings are implemented yet. So from time to time the example files will be updated with new supported index settings. • There are no read permission of some entities, subentities or fields to the rest user. • Product 360 Server is running without variants although the search index configuration is based on variants (e.g. it contains the line: <code>entity.Article.parent= Variant</code> and <code>entity.Variant.parent= Product2G</code>). • The search index configuration defines a catalog which is unknown in Product 360. • The search index configuration does not contain an entity definition, such as <code>entity.Variant.pageable=true</code> .
<p>Test of fulltext search on <code>hps-config-admin</code> works but not with Product 360 Web</p>	<ul style="list-style-type: none"> • Check if Product 360 Web Search settings in <code>webfrontend.properties</code> are correct. • Check if Product 360 Web Search server is running
<p>No search results</p>	<p>Please check:</p> <ul style="list-style-type: none"> • Index build was successful. • Product 360 Server and Product 360 Web Server is available • Product 360 - Web Search server is available • Use for the first time an asterix '*' as a search string • Check all index configuration settings in: <ul style="list-style-type: none"> • <code><PIM_WEBSEARCH_INSTALLATION_ROOT>/configuration.properties</code> • <code><PIM_INSTALLATION_ROOT>/webfrontend.properties</code> • <code><PIM_INSTALLATION_ROOT>/fulltextsearch.properties</code> • May be the Product 360 data has not anything which matches the search string
<p>Drill-Down functionality does not work</p>	<p>Please check in the index configuration:</p> <p>Define more than one entity:</p> <pre>entity.Article.pageable= true entity.Variant.pageable= true or entity.Product.pageable= true</pre> <p>Define parent key:</p> <pre>entity.Article.parent=Variant or entity.Article.parent=Product</pre>

Problem	Possible solution
Object rights will not be considered	<p>Object rights of Item-, Variant- and Product2G entities will be automatically added to the index configuration</p> <p>If the customer has additional ArticleType-based entities, add following field definitions to the index configuration: (e.g. entity identifier = EntityBasedOnArticleType)</p> <pre>field.EntityBasedOnArticleType.AclProxy.type=keyword field.EntityBasedOnArticleType.AclProxy.sortable=false field.EntityBasedOnArticleType.AclProxy.filterable=true field.EntityBasedOnArticleType.AclProxy.searchable=true field.EntityBasedOnArticleType.AclProxy.stored=true field.EntityBasedOnArticleType.AclProxy.autocompletable=false</pre>

16 Appendix

16.1 Language Packs

Starting with Product 360 Version 8.0.5 the language packs for the Server, the Desktop and Web client are already part of the installation package. For example, the PIM_8.0.5.00_server_win64.full.zip package already contains all language properties which are available for this release.

You just need to have the corresponding language module activated in your license. Please contact your sales representative for details on how to purchase a language license.

16.2 Standard Classification Systems

Find an overview on the installation scripts for standard classification systems available for Product 360 in the table provided below

The different versions of these systems are available in specific languages only.

Except some versions of ECLASS the installation scripts are available for both DB platforms MS SQL Server and Oracle.



The existing standard classification system scripts are no longer actively supported for new versions of Product 360. Please contact Informatica Professional Service (IPS) team or your partner to assist with your requirements.

AVAILABLE CLASSIFICATION SYSTEMS								
Classification System	DE	EN	FR	IT	ES	CZ	ZH	NL
ECLASS-4.0	X	X			X			
ECLASS-4.1	X	X	X	X	X	X		
ECLASS-5.0.1	X	X	X					
ECLASS-5.1	X	X	X	X	X		X	
ECLASS-5.1.1	X							
ECLASS-5.1.2	X	X						

ECLASS-5.1.3	X							
ECLASS-6.0	X	X						
ECLASS-6.1	X	X						
ECLASS-7.0	X ¹							
ECLASS-7.1	X ¹							
UNSPSC-8.12.01		X						
UNSPSC-9.12.01		X						
UNSPSC-10.12.01		X						
UNSPSC-11.05.01		X						
ETIM 2.0	X	X						
ETIM 3.0	X	X						
ETIM 4.0	X	X						
ETIM 5.0	X	X						X

¹ Scripts for MS SQL Server available only

16.2.1 Download

Please contact the Informatica Support team if you want to use one of these standard classification systems and need the corresponding scripts.