Informatica® MDM - Supplier 360
10.4

Installation and Configuration Guide

Informatica MDM - Supplier 360 Installation and Configuration Guide
10.4
March 2020

Publication Date: 2022-07-26

Table of Contents

Preface

Follow the instruction in *Informatica MDM - Supplier 360 Installation and Configuration Guide* to install and upgrade Informatica MDM - Supplier 360. The guide also includes pre-installation and post-installation tasks and pre-upgrade and post-upgrade tasks.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Introduction to Informatica MDM - Supplier 360

This chapter includes the following topics:

Informatica MDM - Supplier 360 Application Overview

Informatica MDM - Supplier 360 provides clean, consistent, and connected information about suppliers. Business managers use this master supplier data to make better business decisions about suppliers and to implement processes that can save the organization money.

With Supplier 360, business users can achieve the following goals:

- Automate supplier applications and profile maintenance with the Supplier Portal.
- Streamline the supplier onboarding and approval processes.
- Centralize data about suppliers in a master database.
- Enrich supplier data with related information, such as compliance documents, for a true 360 degree view of a supplier.
- Reflect relationships among suppliers, parent companies, subsidiaries, and subsuppliers.
- Alert business managers to existing and upcoming compliance issues.
- Analyze suppliers based on attributes, such as performance, location, products, services, and invoices.
- Connect supplier data with the supplier product catalogs.
- Distribute trustworthy supplier data to business applications and analytical applications across the organization.

Supplier 360 is an application designed for Informatica Multidomain MDM. Business users connect to master supplier data through a business-friendly user interface, which displays an enterprise-level dashboard as well as 360 degree supplier views that are customized for different business users.

You can add optional products to your Supplier 360 environment. When the environment includes a product information management system, such as Informatica Product 360, suppliers can remotely upload product catalogs to the Product Information Management (PIM) system. When the environment includes Data-as-a-Service, all supplier contact information goes through a validation process.

Supplier 360 contains the following components:

- Supplier Relationship Management
- Supplier Portal
- Product Information Management Integration

Example

A global automobile manufacturer experiences multiple issues with its supply chain. The management team has poor insight into everything from the total spend with a supplier to supplier performance.

Total spend is virtually impossible to assess. The manufacturer has hundreds of suppliers, and the supplier information is dispersed across multiple systems in different geographic areas. The same supplier can be in the systems under slightly different supplier names. The manufacturer holds multiple locally negotiated contracts with a supplier. Without a complete picture, the contract terms do not reflect the total spend with a supplier.

The management team does not have insight into supplier overall performance, such as the percentage of orders delivered on time over the last year. Therefore, managers do not take action to resolve performance issues. Late or incomplete shipments of parts continuously affect the supply chain. In some cases, managers have not lined up alternative suppliers for parts, so when parts are unavailable from one supplier, the manufacturing line falters.

Finally, the organization is acquiring another company later in the year. The management team wants a solution in place before that acquisition completes.

Informatica Solution

The IT department implements Supplier 360. An administrator loads data from source systems into Supplier 360, which includes a centralized database for master supplier profiles. Within the centralized database, the application identifies potential duplicate suppliers.

Data stewards review potential duplicate suppliers and merge the supplier profiles as appropriate. Data stewards edit supplier profiles and set up supplier relationships by identifying parent companies and their subsidiaries. Whenever a data steward modifies a record that is part of a supplier profile, the data steward sends the record for review through an online business process.

With the reviewed and approved master data in place, data stewards send invitations to all qualified suppliers to register on the Supplier Portal. Registered qualified suppliers can update their information, add product catalogs, and monitor their performance. Other suppliers use the Supplier Portal to apply to become a supplier to the organization. Online application forms go through an online onboarding and qualification process.

Managers participate in reviews of supplier applications and monitor supplier performance and compliance. When business managers identify compliance and performance issues, they create alerts to notify suppliers of the issues. Managers edit supplier profiles and initiate a change-approval review from the Data workspace. Managers identify alternative suppliers for all key parts and invite the suppliers to complete an online application through the Supplier Portal.

Results

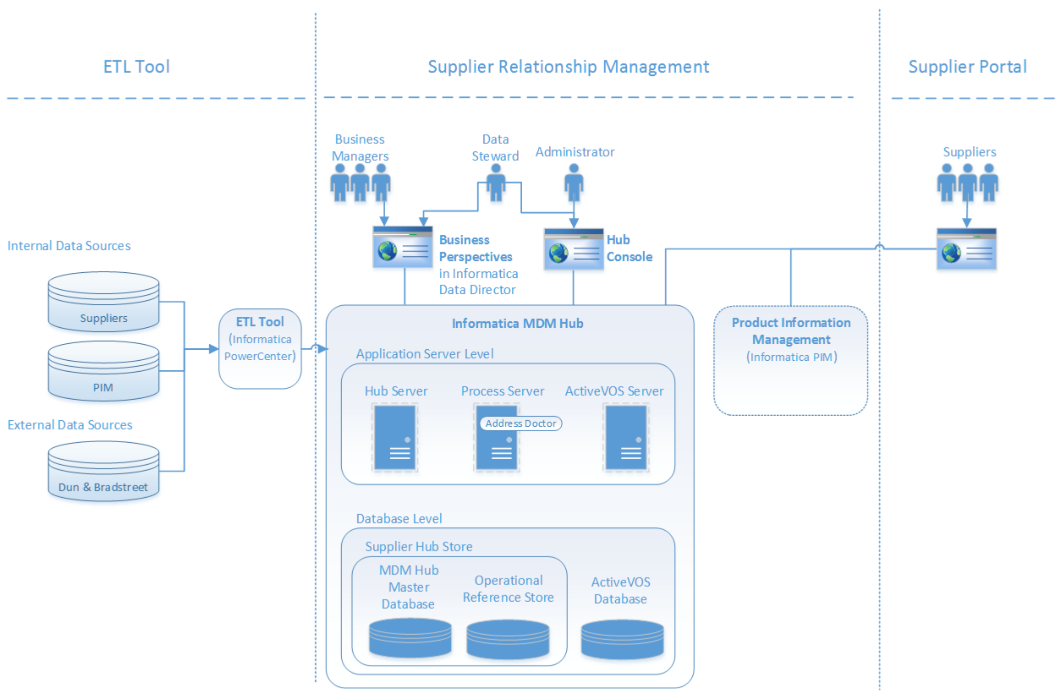
Within the first year, the organization realized savings in the following areas:

- Saved on purchase prices by negotiating with suppliers to provide single favorable contracts for all locales, including volume discounts and early payment discounts
- Reduced costly delays in the supply chain by using alternative suppliers for parts and by monitoring and correcting supplier performance
- Reduced administrative costs by implementing a self-service approach for new suppliers to apply online and for existing suppliers to maintain their supplier data online
- Reduced administrative costs by using an automated business process for the qualification workflow
- Reduced the costs of integrating supplier data after the acquisition by adding the acquired systems as source systems to the MDM Hub

Architecture

The Application requires Multidomain MDM with Data Director and the embedded Informatica ActiveVOS Server. For mapping data, you can use any ETL product, such as Informatica PowerCenter. For product catalogs, you can use any Product Information Management system, such as Informatica Product 360.

The following diagram shows Supplier Relationship Management in the center and the Supplier Portal to the right. The inputs to the MDM Hub are internal and external data sources. A PIM system is optional.



Supplier Management

Supplier 360 adds features to the Informatica MDM environment, such as a database schema for supplier data, business processes for supplier management, and an interface that business users use to access supplier data.

Supplier relationship management includes approval of a supplier, supplier profile management, and assessment of the supplier performance.

Informatica Multidomain MDM

Supplier Relationship Management includes the standard Informatica MDM components:

Hub Store

Databases that store and consolidate business data. The Hub Store consists of an MDM Hub Master Database and Operational Reference Stores. The Application ships with a database schema that you use to create an Operational Reference Store for supplier master data.

Hub Server

A J2EE application that you deploy on an application server. The Hub Server processes data within the Hub Store and integrates the MDM Hub with external applications. The Hub Server is the run-time component that manages core and common services for the MDM Hub. It also manages user authentication across all components.

Process Server

A J2EE application that you deploy on an application server. The Process Server cleanses and matches data and performs batch jobs such as load, recalculates best version of the truth, and revalidates. The Process Server interfaces with cleanse engines to standardize the data and to optimize the data for match and consolidation.

ActiveVOS Server

Business process management software that automates business processes. The Application ships with business processes that help you to manage the supplier lifecycle. These processes ensure that authorized business managers review supplier applications and review internal updates to master data.

Data Director

A browser-based interface that business managers use to view and manage data. The Application ships with Supplier 360, which contains an enterprise-level Start workspace focused on suppliers and customizable Entity 360 views designed for business managers.

Hub Console

A browser-based interface that administrators use to manage the MDM Hub and data stewards use for managing records and batch processing of records.

Supplier Portal

The Supplier Portal is a web application that you implement in a public-facing website. Suppliers use the Supplier Portal to initiate and maintain a supplier relationship with your organization.

The Supplier Portal requires that users log in. The MDM Server manages user authentication through its Security Access Manager.

Product Information Management Integration

Product Information Management (PIM) systems create a single repository for all product data. In Supplier 360, a PIM system is an optional component. When the Application environment includes a PIM system, suppliers can upload their product catalogs from the Supplier Portal.

When Product 360 is pre-installed, the Application integrates Informatica MDM and the Supplier Portal with Product 360 through an MDM-PIM adapter. The MDM Hub Server manages user authentication with Product 360 through its Security Access Manager and a customized security provider.

If you want to integrate the Application with a third-party PIM system, contact your Informatica representative. Your representative can request the customization of the MDM-PIM adapter for the third-party PIM system.

Supplier Data Models and Database Schema

You configure an Operational Reference Store to use a database schema designed for supplier data. The Application ships with a conceptual data model, a logical data model, and the database schema.

Conceptual Data Model for Supplier Data

The conceptual data model presents the entities, attributes, and relationships for supplier data.

Logical Data Model for Supplier Data

The logical data model presents the structure of the Operational Reference Store for supplier data, including the tables, columns, foreign key relationships, and lookups.

Database Schema for Supplier Data

The database schema contains the base object tables, staging tables, and other elements required to create the schema for supplier data. You have a choice about whether you start the implementation with empty tables or whether you start with reference data. If you use the reference data, some of the repository tables are set up for you.

You can find the data model diagrams and a description of the database schema in the distribution package.

User Roles

MDM Hub user roles control read and write privileges in the Operational Reference Store that contains the supplier master data.

The application has the following MDM Hub user roles:

User roles for system users

User roles for system users include Application Administrator, Portal Administrator, Data Steward, and Data Entry Operator. The Application Administrator role is for a super user, who has full privileges. The Portal Administrator role has administrative privileges on the Supplier Portal.

User roles for business users

User roles for business users control the data privileges in the Operational Reference Store and also the review privileges in business processes. Each business user who is authorized to participate in supplier management receives one or more role assignments. Many people can have the same role.

Supplier 360 includes predefined roles for the following business users:

- Commodity Manager
- Finance Manager
- Contracts Manager
- Compliance Manager

User roles for the Supplier Portal

User roles for the Supplier Portal control which pages can be edited and by whom. When an authorized supplier representative edits a page, the data in the Operational Reference Store is updated.

Supplier 360 includes the following predefined roles in the MDM Hub:

- Supplier Administrators
- Supplier Users

Business Processes for Supplier Management

Business processes help you automate some common supplier lifecycle management workflows.

The Application ships with ActiveVOS business processes for the following workflows:

- Create a supplier (initiated from the Supplier Portal)
- Create or update a supplier profile (initiated from Supplier 360)
- Delete a supplier (initiated from Supplier 360)

For more information about the business processes, see the chapter on *Business Processes for Supplier Management*.

Supplier Profile

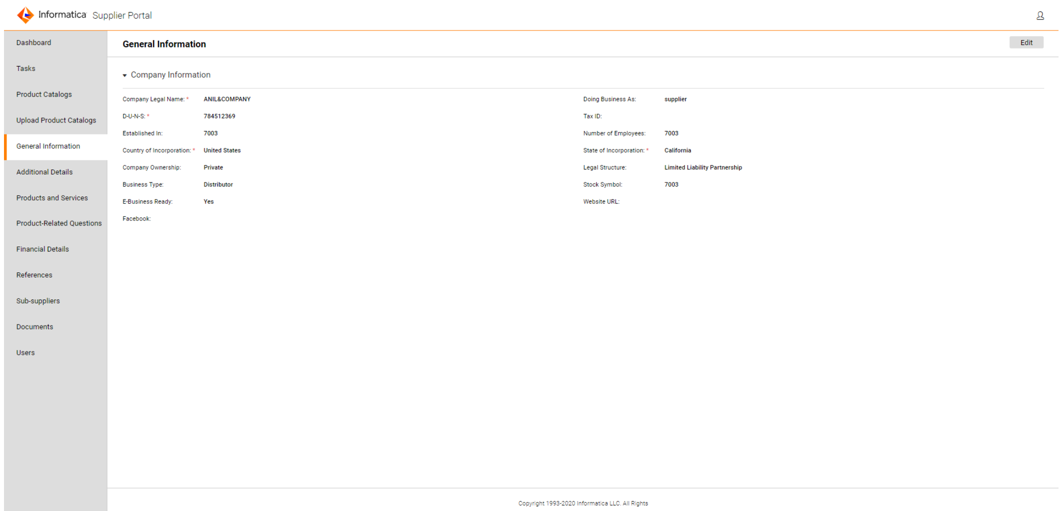
After a supplier is approved, the supplier application is converted to a supplier profile. The supplier profile contains all the information from the application.

Supplier representatives use the Supplier Portal to view their supplier profile. When a supplier representative signs on to the Supplier Portal, the representative sees the Welcome dashboard. In the left navigation panel under Company, the links summarize the information that makes up the supplier profile. In the display area, the representative can see messages, links to catalogs, notifications, renewal alerts, invoices, and some performance metrics. Authorized supplier representatives can modify information, add supporting documentation, upload catalogs, and monitor performance.

Business users use Supplier 360 to open and view supplier profiles. A data steward can edit data in the supplier profile, send notifications to the supplier, and change the status of a supplier. A data steward can also create supplier profiles.

If the Supplier Portal connects to a Product Management Information (PIM) system, the product catalog upload and product catalog management operations are available to the suppliers. The supplier must have the necessary permissions to upload and edit product catalogs.

The following image shows the Supplier Portal user interface when the environment integrated with Product 360:



Storage for Supplier Documents

When the Operational Reference Store resides in an Oracle database or a Microsoft SQL Server database, you can upload documents to the Operational Reference Store. Documents can include proof of insurance, certifications, or any other documentation required by your organization.

You can upload documents in any of the following file formats: .pdf, .doc, .png, and .jpg. The Operational Reference Store stores the files as blobs (binary large objects) and the metadata about the stored files resides in a FILE_METADATA table, which is a child table of the party base object (PARTY_BO).

Supplier 360

Business managers use Supplier 360 to access supplier master data. Supplier 360 runs in Informatica Data Director and acts on the supplier records stored in the Operational Reference Store that contains supplier data.

Business managers can view enterprise-level information about suppliers and view 360 degree information about a supplier. From the Start workspace, managers participate in the review process and monitor all suppliers. From the Data workspace, managers can edit supplier profiles, change the status of a supplier profile, create alerts that appear in the Supplier Portal, and launch the Entity 360 views. From the Entity 360 views, managers monitor supplier compliance and monitor supplier performance. After editing a supplier profile, the manager can initiate a business process where other business managers review and approve the edits.

Online Supplier Application Form

When a supplier wants to become a supplier to a buyer organization, the supplier registers on the Supplier Portal and completes an online supplier application form. The application form prompts the supplier to provide all the information that the buyer requires to begin a qualification process. Each page of the application focuses on a different type of information, such as general company information or banking information.

As a supplier representative fills out the application through the Supplier Portal, the MDM Hub stores the records that make up the application in a pending state in the Operational Reference Store. After the supplier representative submits the application, the application goes through a business approval process. If business users approve the application, the supplier becomes an approved supplier and the application becomes the supplier profile. In the Operational Reference Store, the state of the profile records changes from pending to active. The MDM Hub links the records to construct a 360 degree supplier profile.

The data from the application is now the official supplier profile.

Supplier Profile Maintenance

Approved suppliers use the Supplier Portal to manage their supplier profile.

Authorized supplier representatives can add contacts, monitor delivery performance, receive notifications, and keep data and certifications up-to-date. If the application environment includes a Product Information Management (PIM) system, a supplier representative can also upload a product catalog to the PIM system.

Product Information Management Integration

When the Supplier 360 environment includes a Product Information Management (PIM) system, suppliers can view their product catalogs from the Supplier Portal. Suppliers can also upload a product catalog to the PIM system from the Supplier Portal.

Supplier 360 Integration with Product 360

Supplier 360 is integrated with Product 360 with a preconfigured adapter. The adapter handles signing into the systems and coordinates activities between Supplier 360 and Product 360.

If you want to integrate Supplier 360 with a third-party product information management system, contact your Informatica representative. Your representative can request the customization of the adapter for the third-party system.

Product Catalogs

When the Supplier 360 environment includes a Product Information Management (PIM) system, suppliers can view and upload their product catalogs from the Supplier Portal.

Business managers can upload catalogs from the PIM system user interface.

CHAPTER 2

Supplier 360 Installation Overview

This chapter includes the following topics:

Installation Overview

The Supplier 360 application requires Multidomain MDM and, optionally, a product information management system, such as Product 360. You must install these products before you install the Application.

You receive Supplier 360 as an archive file. The archive contains configuration files, template files, and a setup script. You edit the configuration files to specify properties that reflect your environment. You also need to replace template files with customized files, such as replacing the placeholder logo file with a file containing your organization logo. Then you can run the setup script.

Installation of Supplier 360 consists of the following steps:

1. Read the Release Notes.
2. Verify the software requirements.
3. Perform the pre-installation tasks.
4. Install the application.
5. Complete the post-installation tasks.

Read the Release Notes

Read the *MDM - Supplier 360 Release Notes* for updates to the installation and upgrade process. You can also find information about known limitations for the release.

Verify Software Requirements

Set up the Multidomain MDM environment before you install Supplier 360.

Perform the following tasks:

1. Review the Product Availability Matrix for Supplier 360 to discover the system requirements and supported versions for products, databases, and application servers. You can find all Product Availability Matrices at https://network.informatica.com/community/informatica-network/product-availability-matrices.
2. Install a supported version of Informatica Multidomain MDM, including Informatica Data Director and the embedded version of Informatica ActiveVOS Server. Follow the instructions in the *Multidomain MDM Installation Guide* or the *Multidomain MDM Upgrade Guide* for your environment.

   Note: When you create the Operational Reference Store, you must use the name `supplier_hub`.
3. If using a PIM system, install a supported version of Product 360 or a third-party PIM product.

   Note: If you want to integrate the Application with a third-party PIM system, contact your Informatica representative. Your representative can request the customization of the MDM-PIM adapter for the third-party PIM system.

Verify Minimum System Requirements

Supplier 360 requires the same system requirements as Informatica MDM.

To use the Supplier Portal, enable cookies in the browser.

For more information about product requirements and supported platforms, see the Product Availability Matrix at: https://network.informatica.com/community/informatica-network/product-availability-matrices.

Installation Topology

You can use Supplier 360 application with or without MDM - Product 360.

Based on your requirements, use one of the following installation topologies:

With Product 360

You can integrate Supplier 360 with Product 360. In this mode, the Supplier portal uses the following Product 360 services:

- Timeline
- Product catalogs
- Tasks view
- Product catalog upload

Without Product 360

You can use Supplier 360 without integrating with Product 360 or any other products.

CHAPTER 3

Before You Install

This chapter includes the following topics:

Extract the Application

You receive the Supplier 360 application as an archive file. Create the following directory structure and extract the contents of the Supplier 360 archive file into it:

```
<MDM Installation Directory>/app/tsr
```

The extracted content contains the following files and folders:

File or Folder Name	Description
batchgroup/	Contains the JAR file for the silent installation process.
bin/	Contains installation, upgrade, and database schema validation utilities.
bpm/	Contains the ActiveVOS email service and the default business processes in a deployable format.
config/	Contains configuration properties files.
datamart/	Contains the datamart service and the chart configurations.
docs/	Contains the Supplier 360 Data Dictionary document.

File or Folder Name	Description
email-config/	Contains the subdirectories that contain the database schema and the configuration files to deploy. Following are the list of the subdirectories: - templates/. Contains the avos-templates and pim-templates subdirectories with email body text templates for ActiveVOS and for Informatica MDM - Product 360. - emailConfig.xml
hub/	Contains the subdirectories that contain the database schema and the configuration files to deploy to Data Director. The folder contains the following sub-folders: - change-xml/. Contains the MDM Hub metadata including components, such as landing tables, lookup tables, staging tables, base objects, and match and merge rules, cleanse functions, component instances, business entities, and business entity services. - cocsconfig/ Contains configuration files for the business entities and business entity services. - delta_change_xml/. Contains the newly added MDM Hub metadata. - entity360config/. Contains copies of the Entity 360 component instance definitions that ship with Multidomain MDM. - idd/. Contains the message and error bundle files. - schema/. Contains the database schema for supplier data and reference data.
images/	Contains placeholder images for a logo and for a background image for the Supplier Portal login page.
lib/	Directory for the external libraries. Copy the JDBC driver files for your database to the lib directory.
localizationScript/	Contains the scripts for localizing labels and error messages.
lookuplocalization/.	Contains files for localization of the lookup tables.
pre_s360_10_4/	Contains the installation package for an upgrade environment that uses the Supplier Portal from a version earlier than 10.4.
pre-install-config/	Contains a sample product hierarchy configuration file.
resources/	Contains the resource bundle.properties files for each of the supported locales.
Supplier Portal/	Contains the preconfigured Supplier Portal that does use Product 360 integration.
SupplierPortalWithProduct360/	Contains the preconfigured Supplier Portal that integrates with Product 360.
upgrade	Contains the library files that support the Supplier 360 upgrade process.
was	Contains file for the Provisioning tool user interface for WebSphere environment.
bundleLocalization.jar	JAR file for localization.
Master Data Management Master Notices	Contains notices for MDM products.

File or Folder Name	Description
`MDMAppsServices.war` and `uiwebapp-ear.ear`	File for Supplier 360 user interface.
`mdmappsview-ear.ear`	Supplier 360 components.
`productversion.jar`	JAR file for the product version.
`provisioning-ear.ear`	Provisioning tool user interface for a JBoss environment.

Create the Operational Reference Store

Create an Operational Reference Store with the schema name `supplier_hub`. When entering database parameters, use the parameters that you specified when you created the Oracle database instance.

Note: You must use the name supplier_hub. If you use a different name, the integration with Product 360 does not work.

1. Navigate to the following directory:

   ```
   <MDM installation directory>/hub/server/bin
   ```

2. Run one of the following commands:
   - On Windows. `sip_ant.bat create_ors`
   - On Linux. `sip_ant.sh create_ors`
3. Enter values for the Operational Reference Store parameters.

   Note: The prompts display default text in brackets. Press **Enter** to use the default value and go to the next prompt.

Parameter	Description
Oracle Connection Type	Enter the type that you specified for the Oracle database instance.
Operational Reference Store DB host name	Enter the IP address of the host running Oracle.
Operational Reference Store DB port number	Enter the port number that Oracle uses.
Operational Reference Store DB service name	If the Oracle Connection Type=service, enter the name of the Oracle service that you specified for the Oracle database instance.
Oracle Net connect identifier	Enter the TNS name that you specified for the Oracle database instance.
Connect URL	Use the default URL unless you are required to change the URL for business reasons or technical reasons.

Parameter	Description
Operational Reference Store DB user name (schema name)	Enter `supplier_hub`.
Operational Reference Store DB user password	Enter a password to assign to the supplier_hub user.
Locale name	Enter the language to use.
DBA user name	Enter the user name for the Oracle database instance.
DBA password	Enter the password for this user.
MDM index tablespace	Use the default value. Creates a tablespace to contain the index components for the Operational Reference Store.
MDM temporary tablespace	Use the default value. Creates a tablespace to contain the temporary components for the Operational Reference Store.
Oracle temporary tablespace	Use the default value. Creates a tablespace to contain the temporary components for the database instance.

The script triggers the process that creates the Operational Reference Store.

4. If the process fails, check the log file for errors:

```
<MDM installation directory>/hub/server/bin/sip_ant.log
```

Import the Database Schema into the Operational Reference Store

After you create the Operational Reference Store, import the database schema from a change list.

After you create the schema, you edit and upload XML files to repository tables. The XML files are required for Supplier 360.

Importing the MDM Metadata

After you create the supplier_hub Operational Reference Store, import the MDM metadata into the Operational Reference Store.

1. Navigate to the following directory:

```
<MDM installation directory>/hub/server/bin
```

2. Run one of the following commands:
   - On Windows. `sip_ant.bat import_ors`
   - On Linux. `sip_ant.sh import_ors`
3. Enter values for the Operational Reference Store parameters.

Note: The prompts display default text in brackets. Press **Enter** to use the default value and go to the next prompt.

Parameter	Description
Database Type	Enter Oracle.
Oracle Connection Type	Enter the type that you specified for the Oracle database instance.
Operational Reference Store DB host name	Enter the IP address of the host running Oracle.
Operational Reference Store DB port number	Enter the port number that Oracle uses.
Operational Reference Store DB service name	If the Oracle Connection Type=service, enter the name of the Oracle service that you specified for the Oracle database instance.
Oracle Net connect identifier	Enter the TNS name that you specified for the Oracle database instance.
Connect URL	Use the default URL unless you are required to change the URL for business reasons or technical reasons.
Operational Reference Store DB user name (schema name)	Enter `supplier_hub`.
Operational Reference Store DB user password	Enter the password for the supplier_hub user.
Locale name	Enter the language to use.
DBA user name	Enter the user name for the Oracle database instance.
DBA password	Enter the password for this user.
Timeline granularity	Enter the timeline units to use. **Note:** After the database schema is imported, you cannot change the timeline granularity.

The script triggers the process that loads the metadata into the Operational Reference Store.

4. If the process fails, check the log files for errors. You can find log files in the following locations:
   - User input errors. `<MDM installation directory>/hub/server/bin/sip_ant.log`
   - Database errors. `<MDM installation directory>/hub/server/bin/<database type>/seed.log`

Registering the Operational Reference Store

Register the supplier_hub Operational Reference Store.

1. Log in to the MDM Hub Console.
2. In the Configuration workbench, click **Databases**.
3. From the main menu, click **Write Lock** > **Acquire Lock**.

4. Click **Register database**.

   The Informatica MDM Hub Connection Wizard starts.

5. Follow the online instructions to specify the same parameters that you specified when you created the Operational Reference Store.
6. On the Summary page, click **Test Database**.

   The Wizard tests the database connection parameters.

7. Ensure that the **Create datasource after registration** check box is selected.
8. Click **Finish**.
9. When prompted, enter the user credentials for the application server.

   The wizard creates a data source.

Importing the Application Metadata

The metadata for the supplier database schema resides in an MDM Hub change list. You import the change list into the Hub Store. The metadata change list creates components, such as landing tables, user exits, lookup tables, staging tables, base objects, and match and merge rules. The created tables are empty.

1. In the Hub Console, in the Configuration workbench, click **Repository Manager**.
2. Click the **Import** tab.
3. Click the button next to the Source field.

   The **Open Repository** dialog box opens.

4. Click **File Repository**.
5. Navigate to the following directory:

   `<MDM installation directory>/app/tsr/hub/change-xml`

6. Select the `SUPPLIER_hub.change.xml` file, and click **OK**.
7. From the Target field, select **supplier_hub**.
8. Select all the schema components and click **Apply**.

   The Repository Manager imports the selected components from the change list.

Inserting Reference Data

After you import the metadata, you can populate the tables with some reference data. By using reference data, you can complete the configuration steps faster, because you do not have to insert the rows into the tables manually.

1. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/tsr/hub/schema/reference-data`

2. Based on your database type, use a database tool to run one of the following scripts:
   - For Oracle. `Supplier_lookup_script_oracle.sql`
   - For Microsoft SQL Server. `Supplier_lookup_script_MSSQL.sql`
   - For IBM DB2. `Supplier_lookup_script_db2.sql`

3. Verify that the lookup records loaded successfully from the Hub Console.
    a. In the Hub Console, in the Utilities workbench, click **Batch Group**.
    b. Expand **BG_All_Lookup_Load** and select **Control & Logs**.
    c. In the Logs for each job table, review the Status column to verify that the load was successful. The Total records column shows the number of records added. The columns to the right of the Total records column displays zeros if all records load successfully.
    d. If the load was unsuccessful, try running the load. Select **BG_All_Lookup_Load** and click **Execute**.

Integrate the MDM Hub with Informatica Address Verification Cleanse Engine

You must integrate the MDM Hub with the Informatica Address Verification cleanse engine for Supplier 360. Use the Informatica Address Verification Adapter for the integration.

For more information about integrating the MDM Hub with the Informatica Address Verification cleanse engine, see *Informatica MDM Multidomain Edition Cleanse Adapter Guide*.

Configuring the Properties Files

Configure the properties files that the install script requires. If you update these properties files in future, you must rerun the install script.

You set properties in the following files:

- `application.properties`
- `mdmapps-config.properties`
- `keystore-pass.properties`
- `mdmapps-log4j.properties`

Configuring the Application Properties File

You must configure the JNDI name of the ActiveVOS data source in the application properties file.

1. Navigate to the following directory:

    `<MDM installation directory>/app/tsr`
2. In a text editor, open the `application.properties` file.
3. In the `activevos.datasource.url` property, configure the JNDI name of the ActiveVOS data source.
4. Save the file.

Configuring the Keystore Properties

Specify the properties related to the keystore in the `mdmapps-config.properties` file.

1. Navigate to the following directory:

   `<MDM installation directory>/app/tsr`
2. In a text editor, open the `mdmapps-config.properties` file.
3. Specify the following properties:

Property	Description
keystore.file.path	Path to keystore.
keystore.pass.property.path	Path to the keystore password file, which is `keystore-pass.properties`.
application.admin.user	Name of the ApplicationAdministrator user that you created.
base.url	Base URL for the business entity services. For example, `http://<Host>:<Port>`

4. Save the file.

Configuring the Keystore Password

Specify the keystore password in the `keystore-pass.properties` file.

1. Navigate to the following directory:

   `<MDM installation directory>/app/tsr`
2. In a text editor, open the `keystore-pass.properties` file.
3. Configure the `keystore.password` parameter.
4. Save the file.

Configuring the Log File Path

Specify the path of the log file in the `mdmapps-log4j.properties` file.

1. Navigate to the following directory:

   `<MDM installation directory>/app/tsr/config`
2. In a text editor, open the `mdmapps-log4j.properties` file.
3. For the `log4j.appender.FILE.File` property, specify the log file name and its path.
   For example, `log4j.appender.FILE.File=/opt/applog/s360/tsr01.log`

   Note: If you plan to install MDM - Customer 360 in the same environment, ensure that you specify a location that is external to both the application. The logs for both the applications are stored in a common file. For example, `log4j.appender.FILE.File=<MDM installation directory>/mdmapplogs/mdmapps01.log`.
4. Save the file.

Configure the Properties File for Silent Installation

If you want to install the Supplier 360 application without user interaction in silent mode, configure the `S360_silent_installer.properties` file. When you perform the silent installation, the installer reads the `S360_silent_installer.properties` file to determine the installation options. Ensure that you provide correct settings in the properties file.

1. Go to the following directory:

   `<MDM installation directory>/app/tsr/config`

2. Open the `S360_silent_installer.properties` file.
3. Set the values for the required parameters in the `S360_silent_installer.properties` file in a text editor.
4. Save the file.

Configuring Email Templates

Some business processes and services send requests to the email service. The email service generates and sends personalized emails to supplier representatives.

To configure email templates, perform the following tasks:

- Edit the email template definitions to add buyer-side email addresses.
- Edit the predefined body text to reflect your organization name, contact information, and Service Level Agreement (SLA) information.

After you install Supplier 360, you configure the email service in ActiveVOS.

List of Email Templates

The email service creates personalized email messages based on email templates. A service request that invokes the email service includes the name of the email template and the values for email template attributes and for body text parameters.

The following table describes the email templates:

Email Template	Description
AfterAcceptSupplier_en	Welcomes the supplier as an approved suppler.
AfterAcceptSupplierInternal_en	Invites a representative from a new supplier to go to the Supplier Portal, register, and fill out an application.
AfterRegistrationSupplier_en	Notifies the supplier representative that the submitted application was received and is under review.
AfterRejectSupplier_en	Notifies the supplier representative that their application was declined.
error_message	Notifies an administrator on the buyer-side when there is an error in the ActiveVOS workflow.

Email Template	Description
OnboardingRegistrationSupplier_en	Notifies the supplier representative that the Supplier Portal registration was successful and describes the next steps.
OnInvitationSupplier_en	Invites a representative from a qualified supplier to register on the Supplier Portal. Used by the buyer after implementing Supplier 360.
ResetPasswordSuccessfulSupplier_en	Notifies the supplier representative that the password was reset successfully.
ResetPasswordSupplier_en	Notifies the supplier representative about the password reset request with the password reset link.
SetPasswordInvitation_en	Welcomes a supplier contact as a user of the Supplier Portal and notifies the user to set password for the user account.
SetPasswordSuccessful_en	Notifies that the supplier contact about the password was reset successfully.
UpdateRequest_en	Notifies the supplier representative that the application has incorrect or insufficient information. The supplier representative can update the application and sent it back for approval.

Email Template Attributes

The `emailConfig.xml` file contains the definitions of the predefined email templates.

In the XML file, the parent `<emailConfigs>` element contains multiple `<emailConfig>` elements, one for each email template. When a service requests an email, it must specify one of these email templates.

The following table describes the attributes that are defined within the `<emailConfig>` element:

Attribute	Value Type	Description
emailTemplate	*template name*	Specifies the name of the email template. The workflow or service that sends the request to the email service specifies which email template to use.
replyTo	*email address*	Specifies a buyer-side email address. This email address receives replies from the supplier representatives.
sendFrom	*email address*	Specifies a buyer-side email address. When a service request does not include an email address to display in the email From field, the email service uses this static email address.
subject	*text*	Specifies the text that appears in the subject line of the email.
template	*XSL template file name*	Specifies the name of the XSL email template that contains the body text for the email.
type	`text/html`	Specifies the format of the email message.

Example Email Template

The following XML sample contains the definition of an email template. When using this template, the email service creates a personalized email that uses the subject line "Supplier Portal - Next Steps" and the body text contained in the RegistrationSuccessful_en.xsl file. The personalized email is sent to the supplier representative.

```
<email-configs>
    <email-config emailTemplate ="registrationSuccessful">
        <replyTo>supplierrelationships@informatica.com</replyTo>
        <sendFrom>supplierrelationships@informatica.com</sendFrom>
        <subject>Supplier Portal - Next Steps</subject>
        <template>RegistrationSuccessful_en</template>
        <type>text/html</type>
    </email-config>
    ...
    </email-configs>
```

Editing the Email Templates

You configure the email templates to add a valid email address that can be used when the service request does not contain an email address. You might also want to add your organization name to the subject line.

1. Navigate to the following directory:

   `<MDM installation directory>/app/tsr/email-config`

2. Open emailConfig.xml in an editor.
3. Search for the <sendFrom> attribute and insert an email address. Repeat for each template.
4. Search for the <replyTo> attribute and insert an email address. Repeat for each template.
5. If you want, search for the <subject> attribute and add your organization name before "Supplier Portal." Repeat for each template.
6. Save the file.

Configure the Body Text in Email Templates

The email templates contain references to .xsl files. The .xsl files contain the body text that is used by the templates. You need to configure the .xsl files.

Different types of text appear in the files:

- Placeholder text, which is enclosed in square brackets, such as [organization name]
- Plain text for the message
- Parameters for personalization which start with <xsl:value-of select=...>

You need to replace placeholder text with your organization name and contact information. You can also edit the plain text and add or remove parameters.

Parameters Used in Email Body Text

When the email service generates a personalized email, it replaces parameters with values that it receives in the service request. For example, a welcome email can include user credentials for the Supplier Portal. Avoid editing these parameters.

The following tables describes the parameters that you can use in body text:

Parameter	Description
<a target="_blank" href="${loginPage}">	Link to the sign in page of the Supplier Portal
<xsl:value-of select="tns:sendEmail/properties/ property[@name='firstName']"/>	First name of a supplier representative
<xsl:value-of select="tns:sendEmail/properties/ property[@name='lastName']"/>	Last name of a supplier representative
<xsl:value-of select="tns:sendEmail/properties/ property[@name='loginName']"/>	User name of a supplier representative, which is the representative's email address
<xsl:value-of select="tns:sendEmail/properties/ property[@name='errorDesc']"/>	Error message

Editing the Body Text

In each XSL file, you need to edit the placeholder text to reflect details about your organization, such as the name and the contact information.

1. Navigate to:

   `<MDM installation directory>/app/tsr/email-config/templates/avos-templates`
2. Open an XSL file in an editor.
3. Search for an opening square bracket ([). Replace the square brackets and the enclosed text with the requested information.
4. Repeat the previous step until you replace all placeholder text.
5. Save the file.
6. Repeat for all other XSL files in this directory.

Integrating Product 360 with Supplier 360

If you want to integrate Supplier 360 with Product 360, you must perform some pre-installation tasks in Product 360. After you install Supplier 360, import the Supplier 360 certificate to the keystore files of Product 360.

Note: If you want to use a third-party PIM product, contact your Informatica representative.

1. Verify the Product 360 keystore files.
2. Activate the Supplier 360 authentication mode for the Product 360 Supplier Portal.
3. Configure the `plugin_customization.ini` file.
4. Set the configuration properties for the Product 360 Supplier Portal.

5. Edit the `webfrontend.properties` file.

Verifying the Product 360 Keystore Files

Ensure that you have keystore files created for the Product 360 Supplier Portal and the Product 360 Server.

Keystore File of the Product 360 Supplier Portal

You can find the details about the keystore file of the Product 360 Supplier Portal in the `configuration.properties` file located in the following directory:

```
<Product 360 Supplier Portal installation directory>/configuration
```

Use the following parameters to verify the keystore file details:

- keystore.location
- keystore.password

The following sample text shows the keystore file details:

```
################################################################################
### Keystore settings

# Defines the file location of the keystore to use
keystore.location = file:D:/Informatica/SupplierPortal/keystore/
supplierPortalKeystore.jks

# Defines the password of the keystore defined via ${keystore.location} property
keystore.password = secret
```

You must also set the `integration.s360.certificate.alias` parameter to infaPortal, which is the alias name of the Supplier 360 certificate that must be added to the keystore file.

The following sample text shows the `integration.s360.certificate.alias` parameter set to infaPortal:

```
################################################################################
### Informatica Supplier 360 integration

# Only used for Informatica Supplier 360 integration
# Informatica Product 360 Supplier Portal provides a authentication method to perform a
login via token verification.
# This property defines the alias of the certificate used to verify the login token.
# The keystore defined with ${keystore.location} needs to contain a certificate with
alias configured by this property.

integration.s360.certificate.alias=infaPortal
```

Keystore File of the Product 360 Server

You can find the details about the keystore file of the Product 360 Server in the `networkConfig.xml` file located in the following directory:

```
<Product 360 Server installation directory>/clusterix/configuration/clusterix
```

The `keyStore` tag contains the keystore file details.

The following sample code shows the keystore file location and the keystore password:

```
<keyStore>
   <file>D:/Informatica/Product360/keystore/p360serverKeystore.jks</file>
   <password>secret</password>
</keyStore>
```

Activating the Supplier 360 Authentication Mode for the Product 360 Supplier Portal

You must activate the Supplier 360 authentication mode named `S360BearerAuth` for the Product 360 Supplier Portal.

1. On Windows, perform the following tasks:
   a. On a command prompt, run the following command:
      `<PIM Supplier Portal directory>\configure.bat`
   b. Add the following argument:
      `-Dspring.profiles.active=S360BearerAuth`
2. On UNIX, perform the following tasks:
   a. In a text editor, open the following script:
      `<PIM Supplier Portal directory>/tomcat/bin/tomcat.sh`
   b. Add the following argument:
      `-Dspring.profiles.active=S360BearerAuth`
   c. Save the file.

Configuring the plugin_customization.ini File

After you configure the authentication mode, update the `plugin_customization.ini` file to enable the authentication mode and configure the keystore alias.

1. In a text editor, open the following file:
   `<Product 360 Server Installation Directory>/server/configuration/HPM/plugin_customization.ini`
2. Configure the following parameters:

   com.heiler.ppm.security.core/S360.authentication.isActive

   Indicates whether to enable the Supplier 360 authentication mode. Set to true.

   com.heiler.ppm.security.core/S360.authentication.keyAlias

   Alias for the keystore file of the Product 360 Server. When you generate the keystore file, you specify the alias for the keystore file.

   com.heiler.ppm.webservice.server/accessTokenExpirationTime.S360

   Validity of the access token that the Supplier 360 authentication mode generates in seconds. Default is 86400.

Set Configuration Properties in Product 360 Supplier Portal

In the Product 360 (PIM) configuration properties file, set user permissions and set the timeline and notification properties to their default values.

1. At a command prompt, navigate to the following directory:
   `<PIM Supplier Portal directory>/configuration/`
2. Open the `configuration.properties` file in a editor.

3. Set the permissions for the default user roles to the specified values:

   ```
   permissions.portalAdmin=VIEW_IMPORT_MANAGER, MANAGE_SUPPLIER_USER
   permissions.supplierAdmin=START_DRY_RUN
   ```

   Note: If these roles have additional permissions, remove the other permissions.
4. If you want the Supplier Administrator role to edit a catalog in the Supplier Portal, add the following entry to the file:

   ```
   global.permission.itemeditor=EDIT
   ```
5. Verify that the timeline and notification settings are set to default values:

   ```
   # Default values for email notifications of new feed messages
   # Supplier user
   feednotification.supplier.USER_REQUEST=true
   feednotification.supplier.USER_REGISTRATION=false
   feednotification.supplier.TEST_RUN_COMPLETE=true
   feednotification.supplier.IMPORT_RUN_COMPLETE=true
   # Portal user
   feednotification.portal.USER_REQUEST=true
   feednotification.portal.USER_REGISTRATION=true
   feednotification.portal.TEST_RUN_COMPLETE=false
   feednotification.portal.IMPORT_RUN_COMPLETE=true
   feedfilter.type
   ```
6. Save the file.

Edit the webfrontend.properties File

Add the login name and password of the users that you created and then specify the Web client theme that is used with the application.

1. Navigate to the following directory:

   `<PIM installation directory>/server/configuration/HPM/`
2. Open the `webfrontend.properties` file in an editor.
3. To add the supplier users, set the following properties:

Property Name	Description
web.client.hsx.supplier.login	Login name of the supplier user with edit permission.
web.client.hsx.supplier.password	Login password of the supplier user with edit permission.
web.client.hsx.readonly.supplier.login	Login name of the supplier user with read-only permission.
web.client.hsx.readonly.supplier.password	Login password of the supplier user with read-only permission.

4. To set the client theme, set the following property to the specified value:

   `web.client.theme=symphony`
5. Save the file.

Sample Configuration for Users

The following example shows the configuration of users in the `webfrontend.properties` file for access to the PIM Web Item Editor from the Supplier Portal:

```
###########################################################
# Informatica PIM - Supplier Portal Integration           #
```

```
##########################################################
# Login name of HPM user that is used for supplier editor
web.client.hsx.supplier.login=hsx
# Login password of HPM user that is used for supplier editor
web.client.hsx.supplier.password=!!hsx!!

# Login name of HPM user that is used for supplier view
# This user has only read-only permissions
web.client.hsx.readonly.supplier.login=hsx
# Login password of HPM user that is used for supplier view
# This user has only read-only permissions
web.client.hsx.readonly.supplier.password=!!hsx!!
```

CHAPTER 4

Installing the Supplier 360 Components

This chapter includes the following topics:

Installing Supplier 360 Overview

After you finish the preinstallation tasks, install Supplier 360 in console or silent mode. If you want to use the preconfigured Supplier Portal of Supplier 360, install the Portal Configuration tool.

Installing Supplier 360 in Console Mode

When you run the installer script, the installer script installs the Supplier 360 application and deploys the ActiveVOS workflows.

1. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/tsr/bin`

2. Run one of the following scripts:
   - On Windows. `install-tsr.bat`
   - On Linux. `./install-tsr.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
MDM Supplier 360 Application installation directory	Press Enter to use the default path or type the fully-qualified path to the directory that contains the application files.
Application Server	Type the name of the application server in lowercase. Use one of the following values: - weblogic - jboss - websphere
avos console username	Type the user name with administrative privileges to access the ActiveVOS Console.
avos console password	Type the password of the ActiveVOS Console user name.

The script updates the `supplier-ear.ear` file.

4. After you successfully install the Supplier 360 application, ensure that you download and apply EBF-21761.

Note: For more information about applying EBF, contact Informatica Global Customer Support.

Installing Supplier 360 in Silent Mode

You can install Supplier 360 in silent mode without any user interaction. Before you install Supplier 360 in silent mode, ensure that you configure the `S360_silent_installer.properties` file.

1. Open a command prompt, and navigate to the following directory:

`<MDM installation directory>/app/tsr/bin`

2. Run the following command:
   - On Windows. `install-tsr.bat silent <MDM installation directory>\app\tsr\config\S360_silent_installer.properties`
   - On UNIX. `./install-tsr.sh silent <MDM installation directory>/app/tsr/config/S360_silent_installer.properties`

Note: The installer runs in the background. The process can take a while to complete. After the installation is complete, review the messages in the command line to ensure the successful installation of Supplier 360.

3. After you successfully install the Supplier 360 application, ensure that you download and apply EBF-21761.

Note: For more information about applying EBF, contact Informatica Global Customer Support.

Installing the Portal Configuration Tool

Use the Portal Configuration tool to import and customize the preconfigured Supplier Portal or create a custom portal.

1. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/portal/bin`

2. Run one of the following scripts:
   - On Windows. `install-portal.bat`
   - On Linux. `./install-portal.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
Portal Configuration tool installation directory	Press Enter to use the default path or type the fully qualified path to the directory where you plan to install the Portal Configuration tool.
Application server	Type the name of the application server in lowercase. Use one of the following values: - weblogic - jboss - websphere
MDM Hub administrator user name	Type the user name with administrative privileges to access the MDM Hub.
ActiveVOS Console user name	Type the user name with administrative privileges to access the ActiveVOS Console.
Password for the ActiveVOS Console user name	Type the password of the ActiveVOS Console user name.
Product 360 integration status	Indicates whether you want to integrate Supplier 360 with Product 360. Use one of the following values: - yes - no
Product 360 Supplier Portal URL	Type the URL to access the Product 360 Supplier Portal.
Product 360 administrator user name	Type the user name with administrative privileges to access the Product 360 Supplier Portal.

The script installs the Portal Configuration tool. After you install the Portal Configuration tool, you can import the preconfigured Supplier Portal of Supplier 360. For more information about importing the preconfigured Supplier Portal, see "Importing the Preconfigured Supplier Portal" on page 51.

CHAPTER 5

After You Install

This chapter includes the following topics:

Configure the MDM Hub

Perform the following post-installation tasks:

- Add user accounts and assign roles
- Configure the MDM Hub for Product 360

Add User Accounts and Assign Roles for Business Users

User roles for business managers control the data privileges in the MDM Hub and review privileges in business processes. Each data steward and business user who is authorized to participate in supplier relationship management receives one or more role assignments. Many people can have the same role.

To add user accounts and assign roles, perform the following tasks:

1. If the business users who need to use the Supplier 360 do not have MDM user accounts, add a user account for each business user.
2. Assign roles to users.
3. If you added new users, add the new users to the application server.

For more information about users and roles, see the *Multidomain MDM Security Guide*.

Role Privileges

You can assign any of the predefined or custom user roles to a user account.

The following table lists the predefined user roles that you can use and summarizes the role privileges:

Role	Add or edit a supplier profile	Review supplier applications or profile updates	Approve supplier applications or profile updates
ApplicationAdministrator	Yes	Yes	Yes
PortalAdministrator	Yes	Yes	Yes
DataSteward	Yes	Yes	No
DataEntryOperator	Yes	No	No
CommodityManager	Yes	Yes	No
FinanceManager	Yes	Yes	No
ContractsManager	Yes	Yes	No
ComplianceManager	Yes	Yes	Yes
abAdmin	No	Yes	No

If you create a custom user role to provide restricted administrator access to the resources, ensure that you assign the user role with the minimum required resource privileges.

The following table lists the minimum resource privileges required for an administrator user role:

Resources	Read	Create	Update	Delete	Merge	Execute
Lookup Alternate Id Type	Yes	No	No	No	No	Yes
Lookup Business Title	Yes	No	No	No	No	Yes
Lookup Country	Yes	No	No	No	No	Yes
Lookup Electronic Address Type	Yes	No	No	No	No	Yes
Lookup Party Status Type	Yes	No	No	No	No	Yes
Lookup Party Status Value	Yes	No	No	No	No	Yes
Lookup Phone Type	Yes	No	No	No	No	Yes
Lookup Portal User Role	Yes	No	No	No	No	Yes
Lookup Postal Address Type	Yes	No	No	No	No	Yes
Lookup State	Yes	No	No	No	No	Yes
Party	Yes	Yes	Yes	Yes	Yes	Yes

Resources	Read	Create	Update	Delete	Merge	Execute
Party Alternate Identifier	Yes	Yes	No	No	No	Yes
Party Electronic Address	Yes	Yes	No	No	No	Yes
Party Phone Communication	Yes	Yes	No	No	No	Yes
Party Postal Address	Yes	Yes	No	No	No	Yes
Party Relationship	Yes	Yes	No	No	No	Yes
Party Status	Yes	Yes	No	No	No	Yes
Postal Address	Yes	Yes	No	No	No	Yes
AddressStandardization5	Yes		No	No	No	Yes
Hierarchy Manager Profile - Default	Yes	Yes	Yes	Yes	Yes	Yes
Supplier Hierarchy	Yes	Yes	Yes	Yes	Yes	Yes
DNB Domestic Ultimate Parent	Yes	Yes	Yes	Yes	Yes	Yes
DNB Global Ultimate Parent	Yes	Yes	Yes	Yes	Yes	Yes
DNB Immediate Parent	Yes	Yes	Yes	Yes	Yes	Yes
Employs	Yes	Yes	Yes	Yes	Yes	Yes
Organization Address	Yes	Yes	Yes	Yes	Yes	Yes
Package Additional Info Custom	Yes	No	No	No	No	Yes
Package General Info Custom	Yes	No	No	No	No	Yes
Package Party Edit	Yes	Yes	Yes	Yes	Yes	Yes
Package Party Postal Address Edit	Yes	Yes	Yes	Yes	Yes	Yes
Package Party Relationship Edit	Yes	Yes	Yes	Yes	Yes	Yes
Package Postal Address Edit	Yes	Yes	Yes	Yes	Yes	Yes
Package Product Related Ques Custom	Yes	No	No	No	No	Yes
Package Product Related Ques Info Custom	Yes	No	No	No	No	Yes
Package Sub Suppliers Info Custom	Yes	No	No	No	No	Yes
Package Supplier Bank Info Custom	Yes	No	No	No	No	Yes
Package Supplier Certificates Info Custom	Yes	No	No	No	No	Yes
Package Supplier Contacts Custom	Yes	No	No	No	No	Yes

Resources	Read	Create	Update	Delete	Merge	Execute
Package Supplier Insurance Info Custom	Yes	No	No	No	No	Yes
Package Supplier Product Services Info Custom	Yes	No	No	No	No	Yes
Package Supplier References Custom	Yes	No	No	No	No	Yes
Package Supplier Tax Info Custom	Yes	No	No	No	No	Yes
Package User Auth Custom	Yes	No	No	No	No	Yes
Supplier Documents Info Custom	Yes	No	No	No	No	Yes
Other Resources - USER	Yes	Yes	Yes	Yes	No	No

Note: If you do not see the `Package Supplier Product Services Info Custom` resource in the list of resources, use the Security Access Manager workbench of the Hub Console to change the resource status to secure.

Creating User Accounts

If some business users do not have MDM Hub user accounts, create the user accounts.

Before you begin, you might want to review an existing MDM Hub user account to see which authentication type is in use in the Informatica MDM environment.

1. In the Hub Console, in the Configuration workbench, click **Users**.
2. Acquire a write lock.
3. Click the **Users** tab.
4. Click **Add user**.

   The Users tool displays the **Add User** dialog box.
5. Enter a first, middle, and last name for the user.
6. Enter the user name for the user. This is the name entered when the user logs in to the Hub Console.
7. Enter the default database for the user, which is the Operational Reference Store that contains the supplier master data.
8. Enter and verify a password for the user.
9. Choose the type of authentication.
   - Select the **Use external authentication** check box if your MDM Hub implementation uses authentication through a third-party security provider.
   - Clear the **Use external authentication** check box if you want to use the internal authentication in the MDM Hub.
10. Click **OK**.

    The Users tool adds the user to the list of users on the **Users** tab.

Assigning Roles to Business Users

You need to assign the user roles to the business users who are responsible for reviewing applications and edited supplier profiles.

You use the Hub Console to assign user roles. You can follow either a role-first approach or a user-first approach. For a role-first approach, you select a role and then select the users and user groups that you want to associate with the role. For a user-first approach, you select a user or user group and then select roles.

When you connect to the Operational Reference Store, select **supplier_hub**.

1. In the Hub Console, connect to the Operational Reference Store that supports the IDD application.
2. Acquire a write lock.
3. Expand the **Security Access Manager** workbench and click **Users and Groups**.

   The Users and Groups tool opens. You can use a role-first approach, a user-first approach, or a mix to attach roles to users.
4. If you want to follow a role-first approach, click the **Assign Users/Groups to Role** tab.
   a. Select a workflow role.
   b. Click the **Edit** button.
   c. In the **Assign Users to Role** dialog box, select the users and user groups who should have this role.
   d. Click **OK**.
   e. Repeat for each workflow role.
5. If you want to follow a user-first approach, click the **Assign Roles to User/Group** tab.
   a. Select a user or user group.
   b. Click the **Edit** button.
   c. In the **Assign Roles to User** dialog box, select the workflow roles suitable for the user or user group.
   d. Click **OK**.
   e. Repeat for each user or user group who requires workflow roles.

Adding MDM-ActiveVOS Users to the Application Server

When you install and configure Multidomain MDM with the embedded ActiveVOS Server, you must set up container-based authentication in the application server and add a user.

Follow these steps to use the ActiveVOS workflow engine with the MDM Hub:

1. In the application server console, create a trusted user and assign the following roles to the user: abAdmin,abServiceConsumer,abTaskClient,abTrust.
2. To configure ActiveVOS to use MDM Identity Services, follow these steps:
   a. In the ActiveVOS console, select **Admin > Configure Services > Identity Services**.
   b. In the Provider Configuration section, enable the **Enable** check box and select **MDM** from the **Provider Type** list.
   c. On the Connection tab, enter the ActiveVOS workflow engine user password as the MDM connection settings password.
      The ActiveVOS workflow engine user is the user that you specified when you added the ActiveVOS workflow engine to the Workflow Manager tool in the MDM Hub Console.
   d. Click **Update**.

e. Test the connection.
    a. Select the **Test** tab.
    b. In the **User for test** field, enter an ActiveVOS user name.
    c. Click **Test Settings**.

Configure the Hub for the Supplier Portal

When the environment includes Product 360, the MDM Hub manages user authentication among all the application components.

When a supplier uploads product catalogs from the Supplier 360 Supplier Portal to the Product 360 Supplier Portal, the MDM Hub handles user authentication between the portals. A custom user profile provider maps the Supplier Portal user roles to the MDM Hub roles. A login provider authenticates the Supplier Portal users with Product 360. The two providers are packaged in a bundle called `PortalLoginProvider.jar`. You must upload the security provider file from the Hub Console.

Uploading the Security Provider for Product 360

The security provider for Product 360 provides security services, such as authentication and authorization, for users that access the MDM Hub. Use the Hub Console to upload the provider file.

1. In the Hub Console, open the **Configuration** workbench and select **Security Providers**.
2. Acquire a write lock.
3. In the Security Providers tool, right-click **Provider File** and select **Upload Provider File**.
4. Navigate to the following directory:

    ```
    <MDM installation directory>/app/tsr/userprofile-provider
    ```
5. Select the `PortalLoginProvider.jar` file.
6. Click **Open**.

    The Security Provider tool populates the Providers list with the additional provider information. After you upload the provider file, you can remove the original file from the file system.
7. Exit the Hub Console.
8. Stop the application server.
9. Restart the application server.
10. To verify whether the security provider is enabled, perform the following tasks:
    a. In the Hub Console, open the Security Providers workbench.
    b. In the left navigation pane, expand **Providers** > **Authentication Providers (Login Modules)** > **Portal Login Module**.
    c. Check whether the provider is enabled.

Redeploying the Portal Configuration Tool

After you manually restart the application server, redeploy the Portal Configuration tool.

1. At a command prompt, go to the following directory:

    ```
    <MDM installation directory>/app/portal/bin
    ```
2. Run one of the following scripts:

- On UNIX. `redeploy.sh`
- On Windows. `redeploy.bat`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
Portal Configuration tool installation directory	Press Enter to use the default path or type the fully qualified path to the directory where you install the Portal Configuration tool.
Application server	Type the name of the application server in lowercase. Use one of the following values: - weblogic - jboss - websphere
MDM Hub administrator user name	Type the user name with administrative privileges to access the MDM Hub.
Redeploy Portal Configuration tool with Product 360	Indicates whether you want to redeploy the Portal Configuration tool with Product 360. Type `no` if you want to install the Portal Configuration tool without Product 360. Use one of the following values: - yes - no

The script redeploys the Portal Configuration tool.

Configuring the Application Server Properties for the Security Provider

After you upload the security provider file, you must configure the application server properties based on the application server that you use.

1. In the Hub Console, open the Security Providers workbench.
2. Acquire a write lock.
3. In the left navigation pane, expand **Providers** > **User Profile Providers** > **Portal Role Based User Profile Provider**.
4. To add a property, click **Add**.

   The **Add Provider Property** dialog box appears.
5. Enter a property and its value.

   Based on the application server that you use, you can add the required properties one by one.

   The following table lists the JBoss properties and their values that you must add:

Property	Value
app.server.type	jboss
java.naming.factory.initial	org.wildfly.naming.client.WildFlyInitialContextFactory

Property	Value
java.naming.provider.url	remote+http://<Host name of application server>:<Port number>
remote.connectionprovider.create.options.org.xnio.Options.SSL_ENABLED	false
remote.connections	default
remote.connection.default.host	localhost
remote.connection.default.port	<Default port>
remote.connection.default.connect.options.org.xnio.Options.SASL_POLICY_NOANONYMOUS	false

The following table lists the WebLogic properties and their values that you must add:

Property	Value
app.server.type	weblogic
java.naming.factory.initial	weblogic.jndi.WLInitialContextFactory
java.naming.provider.url	t3://<Host name of application server>:<Port number>
java.naming.security.authentication	simple
java.naming.security.credentials	<WebLogic console password>
java.naming.security.principal	<Weblogic console username>
remote.connection.default.port	<Default port>
siperian-client.protocol	ejb
weblogic.security.SSL.ignorehostnameVerification	true

6. Click **OK**.
7. Repeat steps 4 through 6 until you add all the properties.

Configure the Operational Reference Store

Before you start the Application, configure the Operational Reference Store that contains supplier data. You must diable a trigger, truncate the data in a repository table, and review the value of the GETLIST Limit property.

Truncating a Repository Table

If you imported the Oracle database dump, the repository table C_REPOS_RPT_DETAILS contains sample data. You must truncate the data.

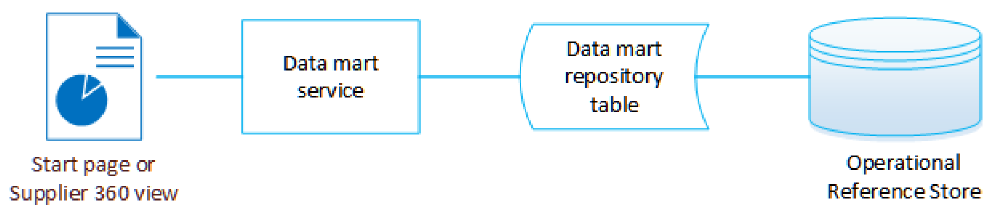
1. In a database tool, connect to the Operational Reference Store for supplier data.
2. Run the following command:

```
truncate table C_REPOS_RPT_DETAILS
```

Populate Supplier 360 Charts with Data

Supplier 360 contains a Home page that contains charts with metrics or data about suppliers. Some of the charts are chart components, and some of the charts are external links. The data for the charts that are available as external links come from a data mart.

The following diagram shows how the data mart works.



The data mart service retrieves data from the Operational Reference Store and stores the results in a repository table. When a Home page loads, the page queries the data mart service for the data and populates the charts.

Note: In the data mart service and configuration files, the term *report* refers to the chart configuration.

To populate the charts that are available as external links, perform the following tasks:

1. Import the chart configurations into a repository table.
2. Configure a database connection between the data mart and the database that contains the Operational Reference Store.
3. Configure the report parameters to include the database name.
4. Populate the data mart with report data.

Chart Configurations for Supplier 360

Supplier 360 ships with predefined chart configurations for the data mart service. Supplier 360 adds chart configurations for supplier data that can be used to populate the charts in the Home page.

The following charts that are available as external links use data mart:

- Documents By Expiry Date
- Supplier By Business Type
- Supplier By Region

Importing the Chart Configurations

To import the configuration of charts that are available as external links, run an insert script on the supplier_hub Operational Reference Store. The script imports the chart configurations into the repository table C_REPOS_RPT_CONFIG.

1. Open a command prompt.
2. Navigate to the following directory:

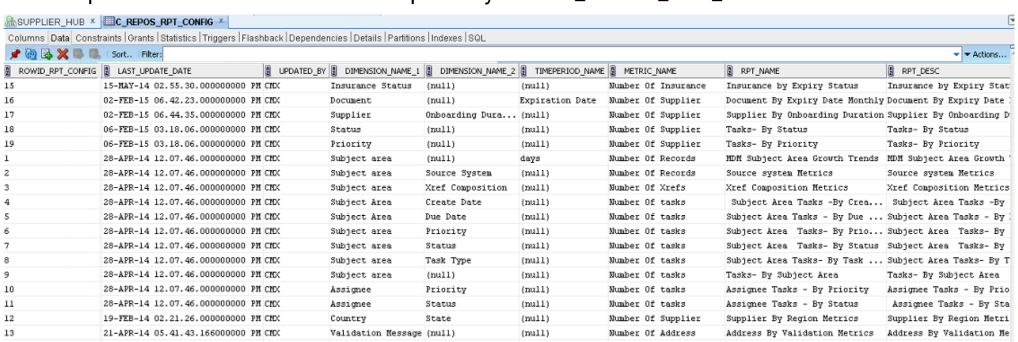
   `<MDM installation directory>/app/tsr/datamart/chart-config`

3. Use a database tool to run the `insert_c_repos_rpt_config.sql` script on the supplier_hub.

   For example, for sqlplus, log in with the Operational Reference Store user name and password and the service name. Then start the script.

   ```
   .../chart-config> sqlplus supplier_hub/password@service
   SQL> @insert_c_repos_rpt_config.sql
   ```

   The script inserts the charts into the repository table C_REPOS_RPT_CONFIG.



SUPPLIER_HUB | C_REPOS_RPT_CONFIG

Columns | Data | Constraints | Grants | Statistics | Triggers | Flashback | Dependencies | Details | Partitions | Indexes | SQL

ROWID_RPT_CONFIG	LAST_UPDATE_DATE	UPDATED_BY	DIMENSION_NAME_1	DIMENSION_NAME_2	TIMEPERIOD_NAME	METRIC_NAME	RPT_NAME	RPT_DESC
15	15-MAY-14 02.55.30.000000000 PM	CMX	Insurance Status	(null)	(null)	Number Of Insurance	Insurance by Expiry Status	Insurance by Expiry Stat
16	02-FEB-15 06.42.23.000000000 PM	CMX	Document	(null)	Expiration Date	Number Of Supplier	Document By Expiry Date Monthly	Document By Expiry Date
17	02-FEB-15 06.44.35.000000000 PM	CMX	Supplier	Onboarding Dura...	(null)	Number Of Supplier	Supplier By Onboarding Duration	Supplier By Onboarding D
18	06-FEB-15 03.18.06.000000000 PM	CMX	Status	(null)	(null)	Number Of Supplier	Tasks- By Status	Tasks- By Status
19	06-FEB-15 03.18.06.000000000 PM	CMX	Priority	(null)	(null)	Number Of Supplier	Tasks- By Priority	Tasks- By Priority
1	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	(null)	days	Number Of Records	MDM Subject Area Growth Trends	MDM Subject Area Growth
2	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	Source System	(null)	Number Of Records	Source system Metrics	Source system Metrics
3	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	Xref Composition	(null)	Number Of Xrefs	Xref Composition Metrics	Xref Composition Metrics
4	28-APR-14 12.07.46.000000000 PM	CMX	Subject Area	Create Date	(null)	Number Of tasks	Subject Area Tasks -By Crea...	Subject Area Tasks -By
5	28-APR-14 12.07.46.000000000 PM	CMX	Subject Area	Due Date	(null)	Number Of tasks	Subject Area Tasks - By Due ...	Subject Area Tasks - By
6	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	Priority	(null)	Number Of tasks	Subject Area Tasks- By Prio...	Subject Area Tasks- By
7	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	Status	(null)	Number Of tasks	Subject Area Tasks- By Status	Subject Area Tasks- By
8	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	Task Type	(null)	Number Of tasks	Subject Area Tasks- By Task ...	Subject Area Tasks- By T
9	28-APR-14 12.07.46.000000000 PM	CMX	Subject area	(null)	(null)	Number Of tasks	Tasks- By Subject Area	Tasks- By Subject Area
10	28-APR-14 12.07.46.000000000 PM	CMX	Assignee	Priority	(null)	Number Of tasks	Assignee Tasks - By Priority	Assignee Tasks - By Prio
11	28-APR-14 12.07.46.000000000 PM	CMX	Assignee	Status	(null)	Number Of tasks	Assignee Tasks - By Status	Assignee Tasks - By Sta
12	19-FEB-14 02.21.26.000000000 PM	CMX	Country	State	(null)	Number Of Supplier	Supplier By Region Metrics	Supplier By Region Metri
13	21-APR-14 05.41.43.166000000 PM	CMX	Validation Message	(null)	(null)	Number Of Address	Address By Validation Metrics	Address By Validation Me
14	21-APR-14 05.41.43.166000000 PM	CMX	Contract Status	(null)	(null)	Number Of Contracts	Contracts by Expiry Status	Contracts by Expiry Stat

Configuring the Data Mart Database Connection

Before you can generate reports or populate charts that are available as external links, you must configure the data mart database connection.

1. Go to the following directory:

   `<MDM installation directory>/app/tsr/datamart/lib`

2. If the directory does not contain the following files, copy them from the `<MDM installation directory>/hub/server/lib` directory:
   - `log4j-1.2.16.jar`
   - `ojdbc7.jar`

- `sqljdbc4.jar`. For Microsoft SQL Server.
- `siperian-common.jar`
- `commons-validator-1.4.0.jar`

3. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/tsr/datamart`
4. Run the following command:
   ```
   java -jar populate_datamart.jar config
   ```
5. At the prompt, type C to configure the database connection.
6. Answer the prompts described in the following table:

Prompt	Description
Connection Name	Enter a unique name for the connection. If the name exists, it will be overwritten.
Type of Connection	Enter the type of connection to the data mart. Currently only DB is supported.
Database vendor	Enter the database to connect with, such as Oracle or IBM DB2 or MS SQL.
User	Enter the database user.
Password	Enter the database password.
Token	Reserved for future use
Host Name	Enter the database host name.
Port	Enter the database port.
Database Name	Enter the database name/SID.

7. When prompted to finish the configuration, enter Y.

   The tool saves the connection information to the `config/mart-population-config.xml` file.

Configuring Parameters

Before you can populate the data mart, you must configure the report parameters for the chart configuration.

You need information contained in other sources.

To find the report names, open the `config/report-class-mapping.properties` file.

To find the configuration IDs, open the C_REPOS_RPT_CONFIG table in a database tool.

1. Open a command prompt.
2. Navigate to the data mart directory.

   `<MDM installation directory>/app/tsr/datamart`
3. Run the following command:
   ```
   java -jar populate_datamart.jar config
   ```
4. Type `P` to configure the report parameters.

5. Answer the prompts described in the following table:

Prompt	Description
Report Name	Specify a report name that appears the `report-class-mapping.properties` file.
Report Configuration ID	Enter the report configuration ID for the report as it appears in the C_REPOS_RPT_CONFIG table.
Mart Connection Name	Enter the connection name for connecting the data mart to an Operational Reference Store. Use the connection name that you defined for the Operational Reference Store that contains the supplier data.
Query Connection Name	Enter the connection name for the database to be queried. - For reports that include the word Tasks, specify the connection name that you defined for the ActiveVOS database. - For all other reports, specify the connection name that you defined for the Operational Reference Store that contains the supplier data.

6. When prompted to finish the configuration, enter N. Add the next table in the list.
7. After you enter all tables, exit the configuration tool.

   The tool saves the parameters to the `config/mart-population-config.xml` file.

Populating the Data Mart with Data

You run a java command to populate the data mart with data for all charts or for a specific chart. If you want to specify a chart, you need to use its report name.

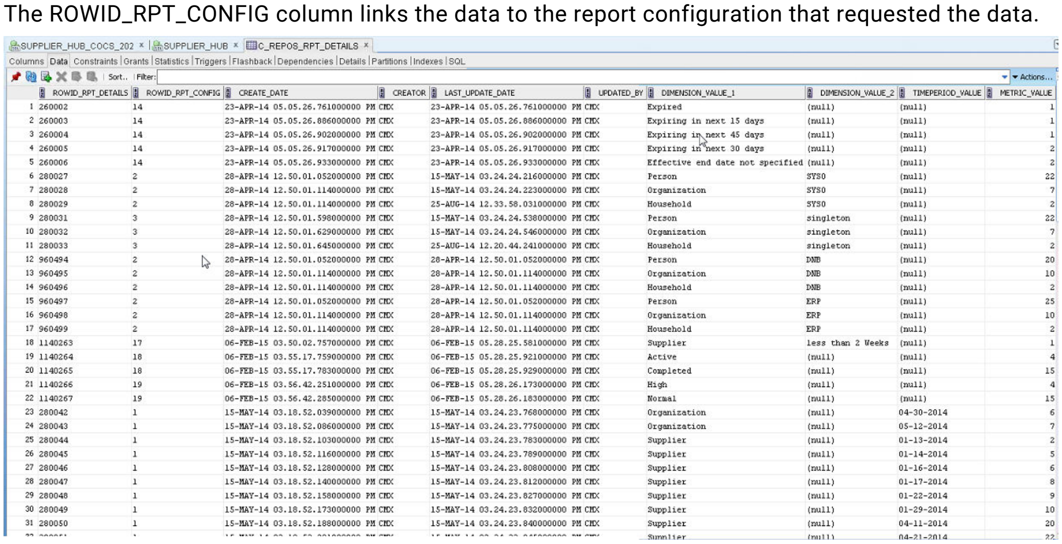
1. Open a command prompt.
2. Run a java command to populate the data mart.
   - To populate the data mart with data for all available reports, run the following command:

     ```
     java -jar populate_datamart.jar
     ```

   - To populate the data mart with data for a specific report, run the following command:

     ```
     java -jar populate_datamart.jar exec <report name>
     ```

If the supplier_hub contains data, the C_REPOS_RPT_DETAILS repository table is populated with report data. The ROWID_RPT_CONFIG column links the data to the report configuration that requested the data.


SUPPLIER_HUB_COCS_202 | SUPPLIER_HUB | C_REPOS_RPT_DETAILS

Columns | Data | Constraints | Grants | Statistics | Triggers | Flashback | Dependencies | Details | Partitions | Indexes | SQL

	ROWID_RPT_DETAILS	ROWID_RPT_CONFIG	CREATE_DATE	CREATOR	LAST_UPDATE_DATE	UPDATED_BY	DIMENSION_VALUE_1	DIMENSION_VALUE_2	TIMEPERIOD_VALUE	METRIC_VALUE
1	260002	14	23-APR-14 05.05.26.761000000 PM	CMX	23-APR-14 05.05.26.761000000 PM	CMX	Expired	(null)	(null)	1
2	260003	14	23-APR-14 05.05.26.886000000 PM	CMX	23-APR-14 05.05.26.886000000 PM	CMX	Expiring in next 15 days	(null)	(null)	1
3	260004	14	23-APR-14 05.05.26.902000000 PM	CMX	23-APR-14 05.05.26.902000000 PM	CMX	Expiring in next 45 days	(null)	(null)	1
4	260005	14	23-APR-14 05.05.26.917000000 PM	CMX	23-APR-14 05.05.26.917000000 PM	CMX	Expiring in next 30 days	(null)	(null)	2
5	260006	14	23-APR-14 05.05.26.933000000 PM	CMX	23-APR-14 05.05.26.933000000 PM	CMX	Effective end date not specified	(null)	(null)	2
6	280027	2	28-APR-14 12.50.01.052000000 PM	CMX	15-MAY-14 03.24.24.216000000 PM	CMX	Person	SYS0	(null)	22
7	280028	2	28-APR-14 12.50.01.114000000 PM	CMX	15-MAY-14 03.24.24.223000000 PM	CMX	Organization	SYS0	(null)	7
8	280029	2	28-APR-14 12.50.01.114000000 PM	CMX	25-AUG-14 12.33.58.031000000 PM	CMX	Household	SYS0	(null)	2
9	280031	3	28-APR-14 12.50.01.598000000 PM	CMX	15-MAY-14 03.24.24.538000000 PM	CMX	Person	singleton	(null)	22
10	280032	3	28-APR-14 12.50.01.629000000 PM	CMX	15-MAY-14 03.24.24.546000000 PM	CMX	Organization	singleton	(null)	7
11	280033	3	28-APR-14 12.50.01.645000000 PM	CMX	25-AUG-14 12.20.44.241000000 PM	CMX	Household	singleton	(null)	2
12	960494	2	28-APR-14 12.50.01.052000000 PM	CMX	28-APR-14 12.50.01.052000000 PM	CMX	Person	DNB	(null)	20
13	960495	2	28-APR-14 12.50.01.114000000 PM	CMX	28-APR-14 12.50.01.114000000 PM	CMX	Organization	DNB	(null)	10
14	960496	2	28-APR-14 12.50.01.114000000 PM	CMX	28-APR-14 12.50.01.114000000 PM	CMX	Household	DNB	(null)	2
15	960497	2	28-APR-14 12.50.01.052000000 PM	CMX	28-APR-14 12.50.01.052000000 PM	CMX	Person	ERP	(null)	25
16	960498	2	28-APR-14 12.50.01.114000000 PM	CMX	28-APR-14 12.50.01.114000000 PM	CMX	Organization	ERP	(null)	10
17	960499	2	28-APR-14 12.50.01.114000000 PM	CMX	28-APR-14 12.50.01.114000000 PM	CMX	Household	ERP	(null)	2
18	1140263	17	06-FEB-15 03.50.02.757000000 PM	CMX	06-FEB-15 05.28.25.581000000 PM	CMX	Supplier	less than 2 Weeks	(null)	1
19	1140264	18	06-FEB-15 03.55.17.759000000 PM	CMX	06-FEB-15 05.28.25.921000000 PM	CMX	Active	(null)	(null)	4
20	1140265	18	06-FEB-15 03.55.17.783000000 PM	CMX	06-FEB-15 05.28.25.929000000 PM	CMX	Completed	(null)	(null)	15
21	1140266	19	06-FEB-15 03.56.42.251000000 PM	CMX	06-FEB-15 05.28.26.173000000 PM	CMX	High	(null)	(null)	4
22	1140267	19	06-FEB-15 03.56.42.285000000 PM	CMX	06-FEB-15 05.28.26.183000000 PM	CMX	Normal	(null)	(null)	15
23	280042	1	15-MAY-14 03.18.52.039000000 PM	CMX	15-MAY-14 03.24.23.768000000 PM	CMX	Organization	(null)	04-30-2014	6
24	280043	1	15-MAY-14 03.18.52.086000000 PM	CMX	15-MAY-14 03.24.23.775000000 PM	CMX	Organization	(null)	05-12-2014	7
25	280044	1	15-MAY-14 03.18.52.103000000 PM	CMX	15-MAY-14 03.24.23.783000000 PM	CMX	Supplier	(null)	01-13-2014	2
26	280045	1	15-MAY-14 03.18.52.116000000 PM	CMX	15-MAY-14 03.24.23.789000000 PM	CMX	Supplier	(null)	01-14-2014	5
27	280046	1	15-MAY-14 03.18.52.128000000 PM	CMX	15-MAY-14 03.24.23.808000000 PM	CMX	Supplier	(null)	01-16-2014	6
28	280047	1	15-MAY-14 03.18.52.140000000 PM	CMX	15-MAY-14 03.24.23.812000000 PM	CMX	Supplier	(null)	01-17-2014	8
29	280048	1	15-MAY-14 03.18.52.158000000 PM	CMX	15-MAY-14 03.24.23.827000000 PM	CMX	Supplier	(null)	01-22-2014	9
30	280049	1	15-MAY-14 03.18.52.173000000 PM	CMX	15-MAY-14 03.24.23.832000000 PM	CMX	Supplier	(null)	01-29-2014	10
31	280050	1	15-MAY-14 03.18.52.188000000 PM	CMX	15-MAY-14 03.24.23.840000000 PM	CMX	Supplier	(null)	04-11-2014	20

Configure the ActiveVOS Email Service

The Application uses the email service available with the ActiveVOS Server. You need to enable the service and specify a mail server.

You configure the email service from the ActiveVOS Console. You can do this step now, while you are configuring the email templates, or you can configure the email service after you install the Application.

Mail Server Properties

When you enable the email service, you need to specify a mail server.

The following table describes the mail server properties that you need to set:

Property	Description
Host	Specify the mail server DNS name or IP address.
Port	Specify the port number to use for communications between the ActiveVOS server and the mail server. The default value is 25.
From Address	Specify the email address to display in the From field of an email. For example, no-reply@example.com.
Username	Specify the name used to log in to the mail server.
Password	Specify the password for the user name.
Security	Optional. Select a security protocol. If you set a security protocol, ensure that the Port you specified supports the protocol.

Configuring the ActiveVOS Email Service

You configure the ActiveVOS email service from the ActiveVOS Console.

If you do not know the location of the ActiveVOS Console or your log in credentials, contact your MDM Hub administrator.

1. Launch the ActiveVOS Console. In a browser, type the following URL, substituting the correct host name and port number:

   ```
   http://[host]:[port]/activevos
   ```
2. Log in to the ActiveVOS Console.
3. Click **Admin**.
4. Click **Configure Services**.
5. Click **Email Service**.
6. Select the **Enable** check box.
7. Specify the properties for your mail server.
8. Click **Update** to save your configuration or click **Update and Test** to save your configuration and send a test mail.

Importing the Supplier 360 Certificate to the Keystore Files of Product 360

You must add the Supplier 360 certificate to the keystore files of Product 360 Server and Product 360 Supplier Portal.

1. On the machine that has Supplier 360 installed, go to the following directory:

   `<MDM Hub installation directory>/hub/server/resource/cert`

2. Copy the `certificate_infaPortal.cert` file to a machine that has Product 360 Supplier Portal installed and to a machine that has Product 360 Server installed.
3. On the machine that has Product 360 Supplier Portal installed, go to the directory that contains the keytool utility.
4. Run the following command:

   `keytool -import -keystore <Keystore file name and its path> -file <Directory containing the copied Supplier 360 certificate>\certificate_infaPortal.cert -alias infaPortal`

   The certificate is imported into the keystore file.

   The following sample command uses `supplierPortalKeystore.jks` as the keystore file:

   ```
   keytool -import -keystore \test\keystore\supplierPortalKeystore.jks -file \test
   \certificate\certificate_infaPortal.cert -alias infaPortal
   ```

   Note: If the certificate already exists, delete the certificate and then import it.

5. On the machine that has Product 360 Server installed, go to the directory that contains the keytool utility.
6. Run the following command:

   `keytool -import -keystore <Keystore file name and its path> -file <Directory containing the copied Supplier 360 certificate>\certificate_infaPortal.cert -alias infaPortal`

   The certificate is imported into the keystore file.

   The following sample command uses `p360serverKeystore.jks` as the keystore file:

   ```
   keytool -import -keystore \test\keystore\p360serverKeystore.jks -file \test
   \certificate\certificate_infaPortal.cert -alias infaPortal
   ```

   Note: If the certificate already exists, delete the certificate and then import it.

Importing the Preconfigured Supplier Portal

If you install the Portal Configuration tool, import the preconfigured Supplier Portal of Supplier 360. Use the Portal Configuration tool to import the Supplier Portal.

1. Open a supported browser.
2. Enter the URL for the Portal Configuration tool.

   The URL has the following format:

   - Secure connections. `https://<MDM Hub Server host name>:<MDM Server port number>/portal-config/`
   - Non-secure connections. `http://<MDM Hub Server host name>:<MDM Server port number>/portal-config/`

   The **Log In** page opens.

3. Enter your user name and password.
4. Click **Log In**.

   The Portal Configuration tool opens and displays the **Home** page.
5. Click **Import Portal**.

   The **Import Portal** dialog box appears.
6. If you want to use the Product 360 components in the Supplier Portal, perform the following tasks:
   a. Navigate to the following directory:

      `<MDM Installation Directory>/app/tsr/SupplierPortalWithProduct360`
   b. Select the `SupplierPortalConfig.zip` file.
7. If you do not want to use the Product 360 components in the Supplier Portal, perform the following tasks:
   a. Navigate to the following directory:

      `<MDM Installation Directory>/app/tsr/SupplierPortal`
   b. Select the `SupplierPortalConfig.zip` file.
8. Select the Operational Reference Store for the portal to use.
9. Select the source system for the portal to use.
10. Enter a unique name for the portal.
11. Click **Import**.

    The selected portal is imported.

Configuring the Default Hierarchy

In the Supplier Dashboard view, the Hierarchies panel displays how a supplier is related to other suppliers or contacts in a hierarchical format. A supplier can belong to multiple hierarchies. If you define a default hierarchy for the hierarchy component, the Hierarchies panel loads the default hierarchy for the supplier. Otherwise, the Hierarchies panel loads the list of hierarchies to which the supplier belongs.

1. In the Provisioning tool, click **Configuration** > **Component Editor**.

   The **Component Editor** appears.
2. Select **LayoutHierarchyComponent** > **HierarchyComponent**.

   The **Properties** panel appears.
3. Edit the XML code as required.

   The following sample code sets Supplier Hierarchy as the default hierarchy:

```
<?xml version="1.0" encoding="UTF-8"?>
<hierarchyComponent
    xmlns="http://www.informatica.com/mdm/HierarchyComponent">
    <defaultHierarchyName>Supplier Hierarchy</defaultHierarchyName>
</hierarchyComponent>
```
4. Click **Apply**.
5. Publish the changes to the MDM Hub.
   a. Click **Publish**.

      A confirmation dialog box appears that prompts you to publish or review the changes.

b. Review the changes or publish without a review.
    - To publish without a review, click **Publish**.
    - To publish after a review, click **Review Changes** and follow the instructions that appear on the screen.

Import the Localized Lookup Data

Supplier 360 installation files include the localized lookup data. If you use a localized environment, import the localized lookup data into the database before you use Supplier 360.

1. Copy the following files from the `<MDM installation directory>/hub/server/lib` directory to the `<MDM installation directory>/app/tsr/lookuplocalization/lib` directory:
    - `log4j-1.2.16.jar`
    - For Oracle. `ojdbc7.jar`
    - For IBM DB2. `db2jcc.jar`
    - For Microsoft SQL Server. `sqljdbc4.jar`
2. Go to the following directory:

    `<MDM installation directory>/app/tsr/lookuplocalization/bin`
3. Run the following command:
    - On UNIX. `./lookup_localization.sh`
    - On Windows. `lookup_localization.bat`
4. At the prompts, enter the following parameters:

Parameter	Description
Database type	Type of database that you use. Use one of the following values: - Oracle - DB2 - MSSQL
User name	User name to access the Operational Reference Store database.
Password	Password for the user name.
Operational Reference Store database host name	Name of the host that runs the Operational Reference Store database.
Operational Reference Store database port number	Port number that the database listener uses.
Database name	For IBM DB2 and Oracle only. Name of the IBM DB2 database or Oracle service.

    The localized lookup data is imported into the staging tables.
5. In the Utilities workbench of the Hub Console, click **Batch Group**.

6. Expand **Localized Lookup Data Load**, and select **Control & Logs**.
7. Click **Execute**.

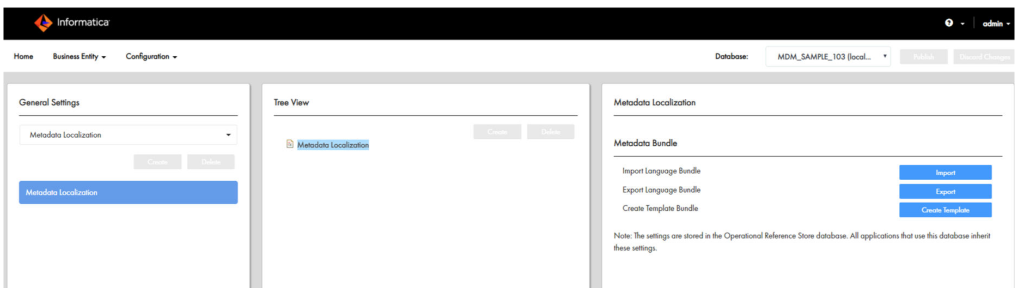
   The localized lookup data is imported into the base objects.

Importing the Localized Metadata

If you use a localized environment, you can import the localized metadata of Supplier 360. Metadata provides additional information about data. For example, metadata for a Supplier business entity includes the supplier's first name, last name, business type, and business name.

1. In the Provisioning Tool, click **Configuration** > **General Settings.**

   The **General Settings** page appears.
2. Select **Metadata Localization**.
3. In the **Metadata Localization** panel, under **Metadata Bundle**, click **Import**.



4. Browse to the following directory:

   `<MDM installation directory>/app/tsr/hub/cocsconfig/`
5. Select the `besMetadata.zip` file, and then click **Open**.

   The localized metadata is imported.

Test Supplier 360

You can log in to Supplier 360 with your administrative user credentials.

Note: The Start workspace contains the Task Inbox and charts. The charts are empty of data until your organization begins adding supplier profiles.

1. Launch Supplier 360:

   ```
   http://<MDM Server host name>:<MDM Server port number>/mdmapps/
   com.informatica.tools.mdm.web.auth/login
   ```
2. Log in with your user credentials.
3. If prompted to select an application, select **Supplier 360**.

   Supplier 360 launches and displays the **Home** page.

Adding Product-Related Questions

The online application form on the Supplier Portal includes a page for product-related questions. You can add questions to this page from Supplier 360.

When you create a product and service, you can define questions specific to the product and service.

1. In Supplier 360, click **New**, select **Products and Services**, and then click **OK**.

   The **Product and Services** page appears.
2. Enter a code for the product and service and a description for it.
3. To relate the product and service to a parent product and service, enter the code for the parent product and service.
4. In the **Questions** section, click **Create Child Record**.
5. Configure the following values.

Field	Description
Question Code	Identifier for the question.
Question Description	Question that you want the suppliers to answer.
Active Indicator	Indicates whether you want the question to be visible to the suppliers.
Answer Type	Type of answer you want to configure for the question. Use one of the following answer types: - Date. Indicates that the answer is a date. - Multi-value. Indicates that the answer can have more than one option. For example, for a confirmatory question, you can have **Yes** and **No** as options. - Text. Indicates that the answer is a text.
Lookup Options	Required only if you select **Multi-value** as the answer type. Comma-separated options for the question. Use the following format: `"Option1,Option2,...OptionN"` For example, "Yes,No"
Mandatory Indicator	Indicates whether the question is a required question.

6. Click **Apply**.
7. To add more questions, repeat steps 4 through 6.
8. Click **Save**.

CHAPTER 6

Business Processes for Supplier Management

This chapter includes the following topics:

Business Processes for Supplier Management Overview

Business processes automate some common supplier lifecycle management workflows.

The Application ships with ActiveVOS business processes for the following workflows:

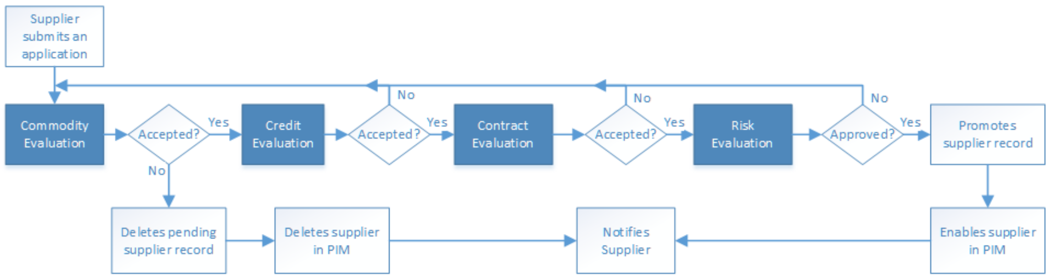
- Create a supplier (initiated from the Supplier Portal)
- Create or update a supplier profile (initiated from Supplier 360)
- Delete a supplier (initiated from Supplier 360)

The following descriptions identify the purpose of each process and identifies the people activities within each process. To view the entire process, open the process in the ActiveVOS Console.

Create a Supplier Process

The `CreateSupplierProcess.bpel` defines a four-step approval process. The process begins when a supplier submits an online application.

The following diagram shows an overview of the process and highlights the people activities.



The first people activity is the commodity evaluation, which requires a commodity manager to review the application. If the commodity manager accepts it, the application moves on to a credit evaluation and then a contract evaluation. The last approval step is a risk evaluation. If the compliance manager believes the risk is acceptable, the manager approves the application and notifies the supplier. At any stage, a manager can reject or send back the application.

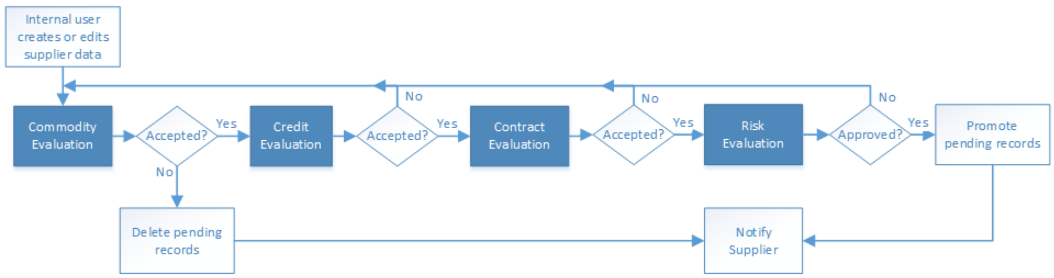
The following table summarizes the people activities within the process, the required role, and the possible actions:

People Activity	Role Assigned	Possible Actions
Commodity Evaluation	CommodityManager	- Accepts the application. This action sends the application onto the Credit Evaluation step. - Rejects the application. This action deletes the pending record containing the changes. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the application to the supplier.
Credit Evaluation	FinanceManager	- Accepts the application. This action sends the application onto the Contract Evaluation step. - Rejects the application with explanation. This action sends the application back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the application to the supplier.
Contract Evaluation	ContractManager	- Accepts the application. This action sends the application onto the Risk Evaluation step. - Rejects the application with explanation. This action sends the application back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the application to the supplier.
Risk Evaluation	ComplianceManager	- Approves the application. This action applies the changes to the master data. - Rejects the application with explanation. This action sends the application back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the application to the supplier.

Supplier Profile Change Approval Process

The default change approval process is a four-step process. The process begins when a business manager creates or edits a supplier profile.

The following diagram shows an overview of the process and highlights the people activities.



The first people activity is the commodity evaluation, which requires a commodity manager to review the update. If the commodity manager accepts it, the update moves on to a credit evaluation and then a contract evaluation. The last approval step is a risk evaluation. If the compliance manager believes the risk is acceptable, the manager approves the update and notifies the supplier. At any stage, a manager can reject or send back the update.

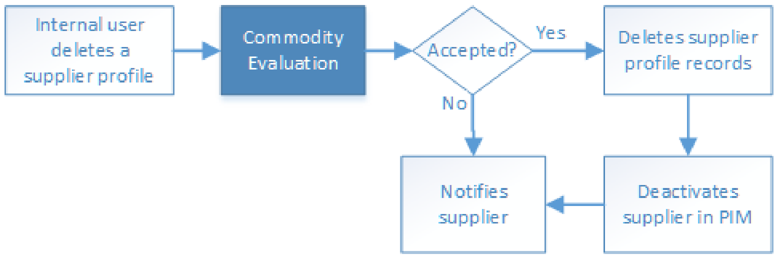
The following table summarizes the people activities within the process, the required role, and the possible actions:

People Activity	Role Assigned	Possible Actions
Commodity Evaluation	CommodityManager	- Accepts the update. This action sends the update onto the Credit Evaluation step. - Rejects the update. This action deletes the pending record containing the changes. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the update to the supplier.
Credit Evaluation	FinanceManager	- Accepts the update. This action sends the update onto the Contract Evaluation step. - Rejects the update with explanation. This action sends the update back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the update to the supplier.
Contract Evaluation	ContractManager	- Accepts the update. This action sends the update onto the Risk Evaluation step. - Rejects the update with explanation. This action sends the update back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the update to the supplier.
Risk Evaluation	ComplianceManager	- Approves the update. This action applies the changes to the master data. - Rejects the update with explanation. This action sends the update back to the Commodity Evaluation step. - Disclaims the task with an explanation so that someone else can claim it. - Sends back the update to the supplier.

Delete a Supplier Internal Process

The `DeleteSupplierProcess.bpel` defines a one-step approval process. The process begins when a business manager deletes a supplier profile.

The following diagram shows an overview of the process and highlights the people activity.



When an internal user attempts to delete a supplier profile, the action is sent to a commodity manager to review.

The following table summarizes the people activity within the process, the required role, and the possible actions:

People Activity	Role Assigned	Possible Actions
Commodity Evaluation	CommodityManager	- Accepts the deletion. This action deletes the supplier profile and notifies the supplier. - Rejects the deletion. This action preserves the supplier profile and notifies the supplier that the deletion was rejected. - Disclaims the task with an explanation so that someone else can claim it.

CHAPTER 7

Customizing Supplier 360

This chapter includes the following topics:

Customizing Supplier 360 Overview

After you configure the Application, you can customize some of the features to better suit your environment. After you customize items, you need to rerun the setup script.

The customization includes extending the data model and customizing the edit privileges for the Supplier Portal pages. If you want to customize other elements of the Application, contact your Informatica representative.

Extending the Data Model

You can extend the Supplier 360 data model by changing the physical schema or by adding types and values to some of the existing tables. You can also add new tables and attributes.

To extend the data model, perform the following steps:

1. Compare your business requirements with the existing schema.
2. List the tables and columns that you want to add.
3. Take a backup of the existing schema.
4. Review the guidelines to extend the data model.
5. Add the tables and columns.

Guidelines for Extending the Data Model

You can modify the definitions of tables or add new tables to the database.

Consider the following guidelines when you extend the data model:

- Check if you can use an existing child base object.
- Do not add a root base object to store the person or organization information.
- Do not define tables with names greater than 24 characters.
- Do not delete existing base objects.
- Do not delete existing columns.
- Do not modify the physical names of existing base objects. However, you can modify the display names.
- Do not modify the data type of an existing column.
- Do not decrease the length of an existing column.
- Prefix the names of the new base object tables to distinguish the tables from the existing tables. The prefix indicates the type of table. Use the following naming convention when you create a base object:

Prefix	Table
C_XO_	Root or child record base object.
C_XR_	Relationship base object.
C_XT_	Lookup base object.

- If you add a column to an existing table, prefix the name of a column with `X_`.

For more information about adding tables and columns, see the *Multidomain MDM Configuration Guide*.

Guidelines for Adding Base Objects

You can add base objects to extend the data model. You can add root or child base objects, lookup base objects, and relationship base objects.

Consider the following guidelines when you add a base object:

- **Child base object with one-to-many relationship**. Use the foreign key from the Party table to relate the table.
- **Child base object with many-to-many relationship**. Use the relationship base object to relate the table to the Party table.
- **Lookup base object**. Set the `LookupIndicator` to true.

Extending the Supplier 360 Resources

Based on the business requirements, you can extend the Supplier 360 resources. For example, to extend business entities, you can create a business entity or a lookup business entity. After you create a business entity, you can add a business entity view. You can also add a child, field, or reference fields to an existing business entity.

Guidelines for Extending the Supplier 360

When you extend the Supplier 360 resources, follow the naming guidelines so that you can distinguish the custom resources from the predefined Supplier 360 resources.

The following table lists the naming guidelines for different Supplier 360 resources:

Resource	Guidelines
Business entity and business entity view	- Add the prefix `Ex` to the names of the new business entities or lookup entities. For example, `Ex<Business Entity Name>`. - Add the prefix `Ex` to the names of the new child, field, or reference field. For example, `Ex<Business Entity Child Name>`. - Do not add a new view to an existing business entity. Create a new business entity, and then add the business entity view.
Relationship type, queries, packages hierarchy, and hierarchy code	Add the prefix `X`.
Staging tables	Add the prefix `C_X`.
Business entity relationships, transformations, business entity service extensions, and component instances, such as layouts and external links	Add the prefix `Ex`.
Cleanse functions	Add the prefix `X`.
Chart components	Add the prefix `X`.

Customizing a Chart

The Home page displays charts that are predefined for Supplier 360. Some of the charts are available as chart components, and some of the charts are available as external links in the Provisioning tool.

The following charts are available as chart components:

- Assigned Tasks By User Roles
- Assigned Tasks By Users
- Closed Tasks By Users
- Contribution By Year
- Open Tasks By Task Type
- Source Systems
- Supplier by Category
- Suppliers Onboarding Time
- Task Priority Overview

- Task Status Overview

The following charts are available as external links:

- Documents By Expiry Date
- Supplier by Business Type
- Supplier by Region

You can customize the charts that are available as chart components to change the chart characteristics or the information the chart shows. You cannot customize the charts that are available as external links. To customize a chart, Informatica recommends that you create a chart component based on the chart that you want to customize and add it to the Home page layout.

For more information about creating a chart component, see the *Multidomain MDM Provisioning Tool Guide*.

Localizing Supplier 360

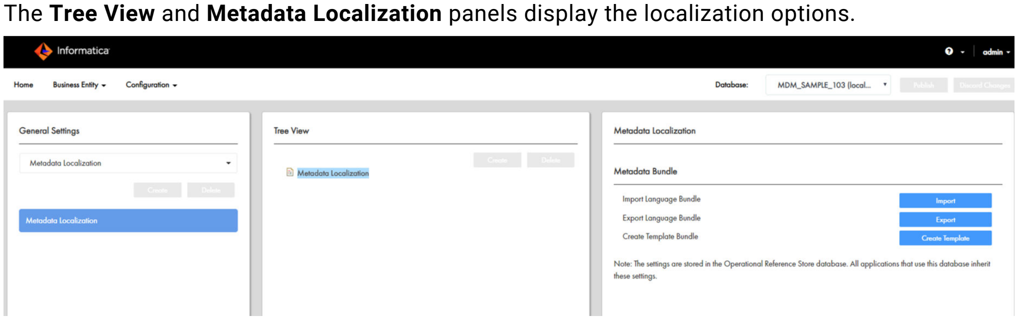
All elements of the user interface in Supplier 360 are localized in the supported languages. You can localize the Supplier 360 resources and custom resources in a language other than the supported languages. The Supplier 360 resources are menus, buttons, navigation links, labels, error messages, and metadata. The custom resources are the business entities, business entity fields, lookup tables, error messages, and labels that you add to customize Supplier 360.

Localizing Metadata

The business entity metadata refers to the resources related to the data model, such as business entity names, menu names, field names, and task types.

1. Click **Configuration** > **General Settings**, and then select **Metadata Localization**.
2. Select **Metadata Localization**.
3. Click **Metadata Localization**.

   The **Tree View** and **Metadata Localization** panels display the localization options.



4. In the **Metadata Localization** panel, under **Metadata Bundle**, click **Create Template**.
5. Save the `besMetadata.zip` file to a location on your local drive.
6. Extract the `besMetadata.zip` file to your local drive.

   The properties files for the selected languages appear.
7. If you want to add a language other than the supported language, save a copy of the `besMetadata.properties` file with the corresponding language code and country code.
   For example, to create the Canadian French version, save the file as `besMetadata_fr_CA.properties`.

8. In a text editor, open the corresponding localized file.
9. For each metadata value, add the localized value in the following format:

   `<Metadata value>=<Localized value>`

   For example, the following property shows a French translated value for the first name:

   ```
   Person.firstName=prénom
   ```
10. Save the changes.
11. Compress the localized properties files to a .zip file named `besMetadata`.
12. In the **Metadata Localization** panel, under **Metadata Bundle**, click **Import**, and then browse to the `besMetadata.zip` file.
13. Click **Open**.

    The language metadata bundle is imported.

Localizing Task Actions, Types, and Messages

Task actions, task types, and task action messages are part of the metadata. Define the task metadata in the `besMetadata.properties` file.

1. Click **Configuration** > **General Settings**, and then select **Metadata Localization**.
2. Click **Metadata Localization**.
3. In the **Metadata Localization** panel, under **Metadata Bundle**, click **Export**. The `besMetadata.zip` template file downloads.
4. Unzip the file, and open the `besMetadata.properties` file in an editor of your choice.
5. Add the task action and task action message properties. Edit the task type properties.

   Use the following syntax for the task properties:

Property Type	Syntax	French Localization Example
Task action	`taskaction.<Task action>=<Localized task action>`	`taskaction.Cancel_Task=Annuler la tâche` **Note:** Replace white spaces in task action names with an underscore. In the example, the white space in `Cancel Task` is replaced with an underscore, `Cancel_Task`.
Task type	`tasktype.<Task type>=<Localized task type>`	`tasktype.AVOSBeMerge=Fusionner` **Note:** To know which task name to add, you must be aware of the predefined MDM workflows that are deployed to the ActiveVOS server as processes.
Task action message	`taskactionmessage.<Task action configuration>.<Task action>=<Localized message>`	`taskactionmessage.TypicalConfig.Escalate=Vous êtes sur le point de transmettre la tâche à votre responsable.`

6. Save the properties file with the appropriate language code and country code suffix.

   For example, to localize metadata in Canadian French, the language code is `fr` and the country code is `CA`. Save the file as `besMetadata_fr_CA.properties`.

7. Compress the properties file.
8. In the **Metadata Localization** panel, under **Metadata Bundle**, click **Import**. The besMetadata.zip template file is imported.

Localizing Lookup Table

A lookup table is a reference table that contains a list of supported values for a column in a base object table. You can localize the lookup tables in any language you want. To localize the lookup tables, create a properties file with the localized values, and then import the localized file into the database.

1. Go to the following directory:

   ```
   <MDM Installation Directory>/app/tsr/lookuplocalization/resources
   ```
2. Save a copy of the lookup.properties file with the language code and country code for the language you want to use.
   For example, to create the Canadian French version, save the file as Lookup_fr_CA.properties.
3. In a text editor, open the localized file you create.
4. For each lookup table value, add the localized value in the following format:

   ```
   <lookup table value>=<Localized value>
   ```
5. Save the file.
6. Go to the following directory:

   ```
   <MDM Installation Directory>/server/lib
   ```
7. Copy the following files:
   - log4j-1.2.16.jar
   - ojdbc7.jar. If you use Oracle database.
   - db2jcc.jar. If you use IBM DB2 database.
   - sqljdbc4.jar. If you use Microsoft SQL Server database.
8. Paste the copied files into the following directory:

   ```
   <MDM Installation Directory>/app/tsr/lookuplocalization/lib
   ```
9. Open a command prompt, and go to the following directory:

   ```
   <MDM Installation Directory>/app/tsr/lookuplocalization/bin
   ```
10. Run the following command:
    - On UNIX. lookup_localization.sh
    - On Windows. lookup_localization.bat
11. At the prompts, enter the following parameters:

Parameter	Description
Database type	Type of database that you use. Use one of the following values: - Oracle - DB2 - MSSQL
User name	User name to access the Operational Reference Store database.

Parameter	Description
Password	Password for the user name.
Operational Reference Store database host name	Name of the host that runs the Operational Reference Store database.
Operational Reference Store database port number	Port number that the database listener uses.
Database name	For IBM DB2 and Oracle only. Name of the IBM DB2 database or Oracle service.

The localized lookup data is imported into the staging tables.

12. In the utilities workbench of the Hub Console, click **Batch Group**.
13. Expand **Localized Lookup Data Load**, and select **Control & Logs**.
14. Click **Execute**.

    The localized lookup data is imported into the base objects.

Mapping the Lookup Tables with the Localized Lookup Tables

All lookup tables support localization. To localize lookup tables, you must map the lookup table to the corresponding lookup localization table. For example, to localize a list of gender codes, map the Lookup Gender lookup table to the Lookup Gender Localized table.

1. In the Provisioning tool, click **Business Entity** > **Modelling.**

   The **Modelling** page appears.
2. Select **Reference Entities**, and then select a lookup entity reference to localize.
   For example, select **LookupGender.**
3. In the properties panel, select **C_BT_GNDR** from the **Base Object** list.
4. Select **Localization**.

   Additional database properties and values appear based on your database table setup.
   The following table contains example values for the properties related to the C_BT_GNDR_LCL localized table:

Property	Value
Base Object	C_BT_GNDR_LCL
Key Column	GNDR_CD
Country Column	CNTRY_CD
Language Column	LANG_CD
Value Column	LOC_STRNG

   Note: When you localize lookup tables, do not configure the same table column as key and value columns. The value column displays the localized value.

5. Publish the changes to the MDM Hub.
   a. Click **Publish**.

      A confirmation dialog box appears that prompts you to publish or review the changes.
   b. Review the changes or publish without a review.
      - To publish without a review, click **Publish**.
      - To publish after a review, click **Review Changes** and follow the instructions that appear on the screen.

Localizing Labels and Error Messages

Labels and error messages are the static texts in the Supplier 360 and Provisioning tool user interface. The text cannot be localized through the Provisioning tool interface. To localize the labels and error messages, edit the Supplier 360 localization bundle files.

1. Go the following directory:

   `<MDM Installation Directory>/app/tsr`
2. Copy the following files:
   - `mdmappsview-ear.ear`
   - `provisioning-ear.ear`
   - `uiwebapp-ear.ear`
3. Paste the copied files into the following directory:

   `<MDM Installation Directory>/app/tsr/localizationScript`
4. Open a command prompt, and go to the following directory:

   `<MDM Installation Directory>/app/tsr/localizationScript`
5. Run the following command:

   `ant extract_all`

   The command extracts the i18n directories containing the localized bundle files for the user interface of Supplier 360 and Provisioning tool.
6. If you want to add a language other than the supported language, go to the following directories, and then save a copy of the `bundle.properties` files in the respective directories with the corresponding language code and country code:
   - `<MDM Installation Directory>/app/tsr/localizationScript/i18n/e360/com.informatica.tools.mdm.client/res/i18n` . For localizing the user interface of the Supplier 360 application.
   - `<MDM Installation Directory>/app/tsr/localizationScript/i18n/uiwebapp`. For localizing the user interface of the Supplier 360 components.
   - `<MDM Installation Directory>/app/tsr/localizationScript/i18n/provisioning`. For localizing the user interface of the Provisioning tool.

   For example, to create the Canadian French version, save the file as `bundle_fr_CA.properties`.
7. In a text editor, open the corresponding localized bundle files, and then update it.
8. From the command prompt, run the following command:

   `ant generate_all`

   The command generates the JavaScript/JSON files for the bundle files.

9. To update the .ear files with the updated localization bundle files, from the command prompt, run the following command:

   ```
   ant update_all
   ```

10. Copy the updated .ear files from the `<MDM Installation Directory>/app/tsr/localizationScript` directory, and then paste the files in the following directory:

    ```
    <MDM Installation Directory>/app/tsr
    ```

11. To localize error messages, user interface labels of external links, and other components on Supplier Dashboard, go to the following directories:
    - `<MDM Installation Directory>/app/tsr/resources/com.informatica.tools.mdm.web.entity360view.childlist`
    - `<MDM Installation Directory>/app/tsr/resources/com.informatica.tools.mdm.web.entity360view.coview.datacomponent`
    - `<MDM Installation Directory>/app/tsr/resources/com.informatica.tools.mdm.web.entity360view.documentlist`
    - `<MDM Installation Directory>/app/tsr/resources/com.informatica.tools.mdm.web.entity360view.externallink`.
12. Add the localized string to the corresponding `bundle.properties` file.
13. Save the file.
14. Go to the following directory:

    ```
    <MDM Hub installation directory>/app/tsr/bin
    ```

15. To deploy the updated `bundle.properties` files, run the following command:
    - On Windows. `install-tsr.bat`
    - On UNIX. `install-tsr.sh`
16. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed Informatica MDM Hub.
MDM Supplier 360 Application installation directory	Press Enter to use the default path or type the fully-qualified path to the directory that contains the application files.
Application Server	Type the name of the application server in lowercase.
Application to deploy	Type `tsr`.
avos console username	Type the ActiveVOS Console username.
avos console password	Type the ActiveVOS Console password.

CHAPTER 8

Upgrading MDM - Supplier 360

This chapter includes the following topics:

Upgrade Overview

To upgrade to MDM - Supplier 360 10.3 HotFix 1, you must first import the database schema from a change list. You must install the Appconfiguration application and verify the global Supplier 360 properties. Then you install Supplier 360.

Extract the Application

You receive the Supplier 360 application as an archive file. Create the following directory structure and extract the contents of the Supplier 360 archive file into it:

```
<MDM Installation Directory>/app/tsr
```

The extracted content contains the following files and folders:

File or Folder Name	Description
`batchgroup/`	Contains the JAR file for the silent installation process.
`bin/`	Contains installation, upgrade, and database schema validation utilities.
`bpm/`	Contains the ActiveVOS email service and the default business processes in a deployable format.
`config/`	Contains configuration properties files.
`datamart/`	Contains the datamart service and the chart configurations.
`docs/`	Contains the Supplier 360 Data Dictionary document.
`email-config/`	Contains the subdirectories that contain the database schema and the configuration files to deploy. Following are the list of the subdirectories: - `templates/`. Contains the `avos-templates` and `pim-templates` subdirectories with email body text templates for ActiveVOS and for Informatica MDM - Product 360. - `emailConfig.xml`
`hub/`	Contains the subdirectories that contain the database schema and the configuration files to deploy to Data Director. The folder contains the following sub-folders: - `change-xml/`. Contains the MDM Hub metadata including components, such as landing tables, lookup tables, staging tables, base objects, and match and merge rules, cleanse functions, component instances, business entities, and business entity services. - `cocsconfig/` Contains configuration files for the business entities and business entity services. - `delta_change_xml/`. Contains the newly added MDM Hub metadata. - `entity360config/`. Contains copies of the Entity 360 component instance definitions that ship with Multidomain MDM. - `idd/`. Contains the message and error bundle files. - `schema/`. Contains the database schema for supplier data and reference data.
`images/`	Contains placeholder images for a logo and for a background image for the Supplier Portal login page.
`lib/`	Directory for the external libraries. Copy the JDBC driver files for your database to the lib directory.
`localizationScript/`	Contains the scripts for localizing labels and error messages.
`lookuplocalization/`.	Contains files for localization of the lookup tables.
`pre_s360_10_4/`	Contains the installation package for an upgrade environment that uses the Supplier Portal from a version earlier than 10.4.
`pre-install-config/`	Contains a sample product hierarchy configuration file.
`resources/`	Contains the resource `bundle.properties` files for each of the supported locales.

File or Folder Name	Description
Supplier Portal/	Contains the preconfigured Supplier Portal that does use Product 360 integration.
SupplierPortalWithProduct360/	Contains the preconfigured Supplier Portal that integrates with Product 360.
upgrade	Contains the library files that support the Supplier 360 upgrade process.
was	Contains file for the Provisioning tool user interface for WebSphere environment.
bundleLocalization.jar	JAR file for localization.
Master Data Management Master Notices	Contains notices for MDM products.
MDMAppsServices.war and uiwebapp-ear.ear	File for Supplier 360 user interface.
mdmappsview-ear.ear	Supplier 360 components.
productversion.jar	JAR file for the product version.
provisioning-ear.ear	Provisioning tool user interface for a JBoss environment.

Configuring the Log File Path

Specify the path of the log file in the mdmapps-log4j.properties file.

1. Navigate to the following directory:

   <MDM installation directory>/app/tsr/config
2. In a text editor, open the mdmapps-log4j.properties file.
3. For the log4j.appender.FILE.File property, specify the log file name and its path.
   For example, log4j.appender.FILE.File=/opt/applog/s360/tsr01.log

   Note: If you plan to install MDM - Customer 360 in the same environment, ensure that you specify a location that is external to both the application. The logs for both the applications are stored in a common file. For example, log4j.appender.FILE.File=<MDM installation directory>/mdmapplogs/mdmapps01.log.
4. Save the file.

Validating the Database Schema

Use the schema validation utility to validate the database schema for any errors. The utility identifies the customized Supplier 360 resources and the custom objects that do not conform to the naming guidelines. Manually fix the errors before you upgrade Supplier 360.

1. Open a command prompt, and go to the following directory:

   `<MDM installation directory>/app/tsr/bin`

2. Run the following command:
   - On Windows. `validate-schema-tsr.bat`
   - On UNIX. `validate-schema-tsr.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
MDM - Supplier 360 installation directory	Press Enter to use the default path or type the fully-qualified path to the directory that contains the application files.
Supplier 360 Operational Reference Store	Database ID of the Supplier 360 Operational Reference Store.
MDM Hub user name	MDM Hub user name to access the Supplier 360 Operational Reference Store.
Password	Password for the user name.

   Note: If you use a WebLogic application server, you are prompted to enter the WebLogic console password.

   The utility validates the database schema. You can find the validation report as an HTML file in the following directory: `<MDM installation directory>/app/tsr/upgrade/report`

4. To validate another database schema, press **y**, and enter the following parameters:

Parameter	Description
Supplier 360 Operational Reference Store	Database ID of the Supplier 360 Operational Reference Store.
MDM Hub user name	MDM Hub user name to access the Supplier 360 Operational Reference Store.
Password	Password for the user name.

5. If you do not want to validate another database schema, press **n**.

Before You Upgrade

Before you upgrade Supplier 360, upgrade the Multidomain MDM installation and back up the Supplier 360 installation files.

1. Before you upgrade to *Multidomain MDM* , ensure that all the users submit the drafts records in Supplier 360.
2. Upgrade the Multidomain MDM installation to a supported version.
3. Back up the Supplier 360 Operational Reference Store.
4. Back up the Supplier 360 library and configuration files.
5. Extract the latest Supplier 360 application archive file.
6. Copy the Supplier 360 configuration files to the `tsr` folder.
7. Configure the application properties file.
8. Configure the base URL for the business entity services.
9. Optionally, if you use the data model based on the Party Role table, migrate to the data model based on the Party table.
10. If you install Customer 360 in the same environment, configure the log file path.
11. If you upgrade Supplier 360 from 10.3 Hot Fix 3, download and apply the EBF-21675.
12. Fix all the errors from the report generated by the validation utility database schema.

Upgrading Supplier 360

You can upgrade Supplier 360 in console or silent mode. Use the silent mode if you do not want any user interaction during upgrade.

Note: When you upgrade from a version earlier than 10.4 , if you use MDM - Customer 360 in the same environment, ensure that you upgrade Customer 360 before upgrading Supplier 360.

Upgrading Supplier 360 in Console Mode

The upgrade utility first validates the database schema that you specify. If the utility finds any errors in the database schema, Informatica recommends that you fix the errors and run the upgrade script again.

After you validate a database schema, upgrade the database schema. You can validate and upgrade multiple database schemas. After you upgrade all the required database schemas, the utility upgrades Supplier 360.

1. Open a command prompt, and go to the following directory:

   ```
   <MDM installation directory>/app/tsr/bin
   ```

2. Run the following command:
   - On Windows. `upgrade-tsr.bat`
   - On UNIX. `upgrade-tsr.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
MDM - Supplier 360 installation directory	Press Enter to use the default path or type the fully-qualified path to the directory that contains the application files.
Application server	Press Enter to use the default path or type the fully-qualified path to the directory where you installed the MDM Hub.
ActiveVOS Console user name	Type the user name with administrative privileges to access the ActiveVOS Console.
Password for the ActiveVOS Console user name	Type the password of the ActiveVOS Console user name.

Note: If you use a WebLogic application server, you are prompted to enter the WebLogic console password.

The utility validates the database schema. You can find the validation report as an HTML file in the following directory: `<MDM installation directory>/app/tsr/upgrade/report`

4. To upgrade the database schema, press **y**.

   The database schema upgrade starts.

5. To validate and upgrade another database schema, perform the following steps:

   a. Press **y**.

   b. Enter the following parameters:

Parameter	Description
Supplier 360 Operational Reference Store	Database ID of the Supplier 360 Operational Reference Store.
MDM Hub user name	MDM Hub user name to access the Supplier 360 Operational Reference Store.
Password	Password for the user name.

   The database schema validation starts.

   c. To upgrade the database schema, press **y**.

   The database schema upgrade starts.

   d. To validate and upgrade another database schema, perform steps a through c.

6. If you do not want to validate and upgrade another database schema, press **n**.
7. To start the Supplier 360 upgrade, press **y**.
8. After you successfully upgrade Supplier 360, download and apply EBF-21761.

   Note: For more information about applying EBF, contact Informatica Global Customer Support.

Upgrading Supplier 360 in Silent Mode

You can upgrade Supplier 360 in silent mode without any user interaction. Before you upgrade Supplier 360 in silent mode, ensure that you configure the `S360_silent_installer.properties` file.

1. Open a command prompt, and navigate to the following directory:

   `<MDM installation directory>/app/tsr/bin`

2. Run the following command:
   - On Windows. `upgrade-tsr.bat silent <MDM installation directory>\app\tsr\config\S360_silent_installer.properties`
   - On UNIX. `./upgrade-tsr.sh silent <MDM installation directory>/app/tsr/config/S360_silent_installer.properties`

   Note: The installer runs in the background. The process can take a while to complete. After the installation is complete, review the messages to ensure the successful upgrade of Supplier 360.

3. After you successfully upgrade Supplier 360, download and apply EBF-21761.

   Note: For more information about applying EBF, contact Informatica Global Customer Support.

Installing the Supplier Portal

The latest Supplier Portal is completely re-engineered and is built with the Portal Configuration tool. If you use the Supplier Portal from an earlier version of Supplier 360, you cannot upgrade your Supplier Portal to the latest Supplier Portal. To continue to use the legacy Supplier Portal, you must install the Supplier Portal.

1. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/tsr/bin`

2. Run one of the following scripts:
   - On Windows. `install-tsr.bat`
   - On Linux. `./install-tsr.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Press Enter to use the default path or type the fully-qualified path to the directory where you installed Informatica MDM Hub.
MDM Supplier 360 Application installation directory	Press Enter to use the default path or type the fully-qualified path to the directory that contains the application files.
Application Server	Type the name of the application server in lowercase.
Application to deploy	Type `portal`.

   The script installs the legacy Supplier Portal.

Installing the Application Configuration Tool

If you use the Supplier Portal from an earlier version of Supplier 360, after you install the Supplier Portal, install the Application Configuration tool.

1. At a command prompt, navigate to the following directory:

   `<MDM installation directory>/app/tsr/bin`

2. Run one of the following scripts:
   - On Windows. `install-tsr.bat`
   - On Linux. `/install-tsr.sh`

3. At the prompts, enter the following parameters:

Parameter	Description
MDM Hub installation directory	Directory where you install the MDM Hub. You can press Enter to use the default path in the script or type the fully qualified path to the directory where you install the MDM Hub.
MDM Supplier 360 Application installation directory	Directory where you install the Supplier 360 application. You can press Enter to use the default path in the script or type the fully qualified path to the directory where you install the Supplier 360 application.
Application Server	Name of the application server. Use lowercase to type the name.
Application to deploy	Application that you deploy. Type `appconfig`.

Configuring the cmxserver.properties File

If you use the Supplier Portal from a version earlier than 10.4, update the `cmxserver.properties` file.

1. Go to the following directory:

   `<MDM installation directory>/hub/server/resources`

2. In a text editor, open the `cmxserver.properties` file.
3. Add the following property and its value:

   ```
   cmx.server.bes.pass-credentials-to-external-call=true
   ```

4. Save the file.

Verifying the Supplier 360 Application Settings

If you use the Supplier Portal from a version earlier than 10.4, verify the Supplier 360 application settings in the Application Configuration tool.

1. Launch Supplier 360 with the following URL format:
   `http://<MDM Server host name>:<MDM Server port number>/mdmapps/com.informatica.tools.mdm.web.auth/login`

2. Log in with your user credentials.
3. If prompted to select an application, select **Supplier 360**.
4. Click **App Configuration**.
5. On the **Connections** tab, re-enter the passwords for all the connection types.
6. Verify other connection parameters.
7. On the **Properties** tab, verify the properties.
8. Click **Save Changes**.
9. Restart the application server.

INDEX

U

W