Informatica® Multidomain MDM
10.3

Upgrading from Version 10.0, 10.1, or 10.2
# Table of Contents

**Preface** ................................. 9

Informatica Resources .................. 9

- Informatica Network .................. 9
- Informatica Knowledge Base ........ 9
- Informatica Documentation .......... 9
- Informatica Product Availability Matrixes ........ 10
- Informatica Velocity .............. 10
- Informatica Marketplace .......... 10
- Informatica Global Customer Support .. 10

**Chapter 1: Upgrade Overview** .......... 11

Introduction ................................ 11

Select an Upgrade Process .............. 12

- Guidelines for Selecting an Upgrade Process .................. 12
- Upgrade Process for a Clean Upgrade (Recommended) .......... 12
- Upgrade Process for an In-place Upgrade .................. 13

Document the Upgrade .................. 14

**Chapter 2: Pre-Upgrade Tasks** .......... 15

Pre-Upgrade Tasks ...................... 15

Prepare for the Upgrade .............. 15

Prepare the Environment .............. 16

Process Existing Jobs .................. 20

Update the MDM Hub Configuration .... 20

- Register the Operational Reference Stores with the Original Schema Owner .......... 21

Prepare the BPM Upgrade .................. 23

**Chapter 3: Database Tasks** .......... 26

Database Tasks Overview .............. 26

Set Up Oracle Database .................. 26

- Step 1. Install and Configure Oracle .................. 27
- Step 2. Set Up Database Instances .................. 27
- Step 3. Set Up Database Privileges and Connections .......... 30
- Step 4. Create the ActiveVOS Schema .......... 30

Set Up Microsoft SQL Server .......... 32

- Step 1. Install and Configure Microsoft SQL Server .......... 33
- Step 2. Create a Microsoft SQL Server Data File Store .......... 34
- Step 3. Install ODBC Driver .......... 34
- Step 4. Create the ActiveVOS Schema .......... 34

Set Up IBM DB2 Database .......... 36
Chapter 4: Application Server Tasks

Application Server Tasks Overview

Set Up JBoss
- Configure Java Virtual Machines
- Configure Server Properties for the Full Profile
- Create the ActiveVOS Console Administrative User
- Start JBoss

Set Up Oracle WebLogic
- Configure the Java Virtual Machines
- Disable WebLogic Server Authentication
- Create the ActiveVOS Console Administrative User

Additional Oracle WebLogic Configuration
- Configuring WebLogic for Standalone Process Server Instances
- Configuring WebLogic for Multiple MDM Hub Master Databases
- Configuring the HTTPS Protocol
- Configuring the JTA Timeout for Informatica Platform

Set Up IBM WebSphere
- Configure Java Virtual Machines
- Encrypt Passwords in the MDM Hub Environment
- Create a Secure Profile in a WebSphere Environment
- Create the ActiveVOS Console Administrative User
- Configure SOAP Request Timeout for MDM Hub Deployments

Additional IBM WebSphere Configuration
- Configuring WebSphere for Standalone Process Server Instances
- Configuring WebSphere for Multiple MDM Hub Master Databases
- Configuring the HTTPS Protocol
- Configuring WebSphere for Informatica Data Director

Chapter 5: Hub Store Upgrade

Hub Store Upgrade Overview

Clone the Hub Store (Clean Upgrade)

Databases Set to a Non-English Locale

Upgrading the MDM Hub Master Database in Verbose Mode

Upgrading the MDM Hub Master Database in Silent Mode

Upgrading Operational Reference Store Databases in Verbose Mode

Upgrading Operational Reference Store Databases in Silent Mode

Confirm that the Upgrade Scripts Ran Successfully
Configure the Hub Server and Process Server Properties.................................. 109
Run the Hub Server PostInstallSetup Script Manually...................................... 109
Run the Process Server PostInstallSetup Script................................................. 110
Register the Operational Reference Stores......................................................... 110
Configure Cleanse Functions for Platform Transformations................................. 115
Validate the Upgraded Metadata........................................................................ 115
Validating Metadata......................................................................................... 116
Saving the Validation Results............................................................................ 116
Resolving Metadata Validation Messages......................................................... 116
Review the MDM Hub Environment Report....................................................... 117
Saving the MDM Hub Environment Report....................................................... 117
Upgrading the SiperianClient Library Classes for the EJB Protocol....................... 118
Prepare the MDM Hub Metadata....................................................................... 118
Upgrade Tests.................................................................................................. 118
MDM Hub Upgrade Tests................................................................................. 119
Custom Code Upgrade Tests............................................................................ 119
Provisioning Tool Upgrade Test...................................................................... 119
Data Director with Business Entities Upgrade Tests........................................ 120
Data Director with Subject Areas Upgrade Tests.......................................... 120
Data Director and Hub Server Properties..................................................... 120
Data Director Global Properties................................................................. 121
Generate the Business Entity Schema.............................................................. 122

**Chapter 10: Search Configuration Upgrade**...................................................... 123
Search Configuration Upgrade Overview....................................................... 123
Step 1. Set Up Elasticsearch........................................................................... 123
  Install Elasticsearch.................................................................................. 124
  Create Keystores, Truststore, and Certificates........................................ 124
  Configure the Elasticsearch Java Virtual Machine (JVM)...................... 125
  Configure the Elasticsearch Properties File........................................... 125
  Secure the Elasticsearch Cluster............................................................ 128
  Upload the Search Guard Configuration to Elasticsearch..................... 129
  Configure the Client Certificate DN in the Elasticsearch Properties File.  129
  Customize the List of Words to Ignore in Searches................................. 129
  Customize the List of Synonyms to Include in Searches........................ 130
  Start Elasticsearch.................................................................................. 130
Step 2. Configure the MDM Hub Properties for Search..................................... 130
  Configure the Hub Server for Search...................................................... 130
  Configure Process Servers for Search..................................................... 131
Step 3. Configure Search by Using the Provisioning Tool................................ 132
  Configure the Elasticsearch Cluster....................................................... 133
  Configure the Search Result Views......................................................... 133
Step 4. Validate the Operational Reference Store........................................... 134
Preface

Welcome to the Multidomain MDM Upgrade Guide. This guide explains how to upgrade your Informatica Multidomain MDM implementation to the most recent version. Ensure you use the Multidomain MDM Upgrade Guide that applies to the version you currently have installed.

This guide is intended for technical specialists who are responsible for upgrading their Informatica Multidomain MDM implementation.

Informatica Resources

Informatica Network


As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- 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 search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.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

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com.
Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access 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. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access 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 augment, extend, or enhance your Informatica implementations. By leveraging any of the hundreds of solutions from Informatica developers and partners, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link: http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.
CHAPTER 1

Upgrade Overview

This chapter includes the following topics:

- **Introduction, 11**
- **Select an Upgrade Process, 12**
- **Document the Upgrade, 14**

Introduction

Thank you for upgrading Informatica Multidomain MDM. You can upgrade directly from the installed version to Multidomain MDM version 10.3.

**Important:** You must upgrade all the MDM components to the same version of Multidomain MDM.

A Multidomain MDM environment can include a development environment, test environment, and production environment. You must upgrade each of these environments. As a best practice, upgrade your development environment first. Identify and resolve any upgrade issues. After you successfully upgrade the development environment, you can upgrade the test and production environments with a high degree of confidence.

**Before You Begin**

Before you begin, ensure that you have the necessary guides and that you review the Product Availability Matrix:

- Ensure that you have the correct upgrade guide for your installed version of Multidomain MDM. On the title page, check the major version number in the title *Upgrading from Version*. Make sure it matches the major version number in the installed product. To find the version number in the installed product, in the MDM Hub Console click **Help > About**. Click **Installation Details**. The version number appears in the release name column. For the purposes of the upgrade, it does not matter whether hotfixes have been applied to the installed product.
- Download the *Multidomain MDM Installation Guide* that applies to your database and application server. To ensure a smooth upgrade, you must perform some of the tasks that are described in the installation guide.
- Review the Product Availability Matrix to learn about changes to the system requirements for this version of Multidomain MDM. You can find the matrix on Informatica Network: [https://network.informatica.com/community/informatica-network/product-availability-matrices](https://network.informatica.com/community/informatica-network/product-availability-matrices).
Select an Upgrade Process

You have the following options for upgrading Multidomain MDM:

**Clean Upgrade (Recommended)**

In a clean upgrade, you prepare a new environment with machines that meet the current MDM system requirements. You clone the MDM Hub Master Database and Operational Reference Stores from the existing environment, copy the cloned databases to the new environment, and run the Hub Store upgrade. You install the Hub Server and Process Servers in the new environment by following the instructions in the *Installation Guide*. For information about planning an infrastructure, see the *Multidomain MDM Infrastructure Planning Guide*.

**In-place Upgrade**

For an in-place upgrade, you update the machines that run Multidomain MDM to be compliant with the current MDM system requirements. Then you upgrade the MDM components.

**Guidelines for Selecting an Upgrade Process**

The type of upgrade determines which type of upgrade process you can choose. In all cases, the clean upgrade is recommended.

The following table lists the types of upgrades and tells you which upgrade process you can use:

<table>
<thead>
<tr>
<th>Type of Upgrade for Multidomain MDM</th>
<th>Clean Upgrade (recommended)</th>
<th>In-place Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade to a major or minor version of MDM</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Upgrade to a hotfix for the installed version of MDM, where the application server has to be updated to a major version to meet the MDM system requirements</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Upgrade to a hotfix for the installed version of MDM, where the application server does not need to be updated to a major version to meet the MDM system requirements</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Upgrade Process for a Clean Upgrade (Recommended)**

The process for a clean upgrade consists of the following phases:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Task</th>
<th>Location of Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Database tasks</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>2</td>
<td>Application server tasks</td>
<td>Upgrade Guide</td>
</tr>
</tbody>
</table>
Upgrade Process for an In-place Upgrade

The process for an in-place upgrade consists of the following phases:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Task</th>
<th>Location of Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Database tasks</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>2</td>
<td>Application server tasks</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>3</td>
<td>Pre-upgrade tasks</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>4</td>
<td>Hub Store upgrade</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>5</td>
<td>Hub Server upgrade</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>6</td>
<td>Process Server upgrade</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>7</td>
<td>Resource Kit upgrade</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>8</td>
<td>Post-upgrade tasks</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>9</td>
<td>ActiveVOS post-installation tasks for the application server</td>
<td>Installation Guide</td>
</tr>
<tr>
<td>10</td>
<td>ActiveVOS post-upgrade tasks for the business entity adapter</td>
<td>Upgrade Guide</td>
</tr>
<tr>
<td>11</td>
<td>ActiveVOS post-upgrade tasks for the subject area adapter</td>
<td>Upgrade Guide</td>
</tr>
</tbody>
</table>

* If there are multiple releases between your installed version and the current version, the best practice is to either do a clean upgrade or review all the pre-installation tasks to ensure that you do not miss any changes that have occurred for the database or application server that you use.
You must capture the details of the Informatica MDM Hub environment before, during, and after you upgrade to verify and, if required, troubleshoot the upgrade. You can provide copies of this information to Informatica Global Customer Support if you require assistance with troubleshooting the upgrade.

The following table describes the sources of upgrade information:

<table>
<thead>
<tr>
<th>Upgrade Information</th>
<th>Source of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Reference Store (ORS) metadata</td>
<td>Validation results from the Repository Manager tool in the Hub Console. Generate the validation results for the ORS metadata before and after the upgrade.</td>
</tr>
<tr>
<td>Upgrade events for the Hub Server and Process Server upgrades</td>
<td>Informatica MDM Hub installer log files</td>
</tr>
<tr>
<td>Hub Server and Process Server information</td>
<td>Hub Server and Process Server log files</td>
</tr>
<tr>
<td>Hub Console information</td>
<td>Hub Console log files</td>
</tr>
</tbody>
</table>

**Related Topics:**
- “Saving the MDM Hub Environment Report” on page 117
Pre-Upgrade Tasks

This chapter includes the following topics:

- Pre-Upgrade Tasks, 15
- Prepare for the Upgrade, 15
- Prepare the Environment, 16
- Process Existing Jobs, 20
- Update the MDM Hub Configuration, 20
- Prepare the BPM Upgrade, 23

Pre-Upgrade Tasks

Whether you perform a clean upgrade or an in-place upgrade, perform the pre-upgrade tasks to ensure your environment is properly configured.

Prepare for the Upgrade

Perform the following tasks to prepare for the upgrade:

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read the Release Notes</td>
<td>The Release Notes contain information about updates to the installation and upgrade process. Important: Some versions of application servers and databases have known limitations when running Multidomain MDM. Ensure that you perform all suggested workarounds.</td>
</tr>
<tr>
<td>Get the latest license file</td>
<td>Request the latest license file when you request the upgrade software for Multidomain MDM.</td>
</tr>
<tr>
<td>Upgrade Task</td>
<td>Details</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Review the upgrade restrictions</td>
<td>Review the following conditions before you begin the upgrade:</td>
</tr>
<tr>
<td></td>
<td>· All the components of the Multidomain MDM implementation must be the same version.</td>
</tr>
<tr>
<td></td>
<td>· If you have multiple versions of Multidomain MDM, each version must be installed in a separate environment. Different versions of Multidomain MDM cannot coexist in the same environment.</td>
</tr>
<tr>
<td></td>
<td>· You must not make any major changes to your environment while you upgrade Multidomain MDM. For example, do not upgrade the Oracle, IBM DB2, or Microsoft SQL Server database during the upgrade process.</td>
</tr>
<tr>
<td></td>
<td>· You must upgrade your Operational Reference Store (ORS) using the upgrade scripts provided. The Repository Manager is not intended to be used as an upgrade tool because some of the artifacts might not be carried over or might be carried over incorrectly from one version to another. For more information, see the Multidomain MDM Release Notes.</td>
</tr>
<tr>
<td>Create an upgrade documentation folder</td>
<td>Create a folder named upgradedoc to store copies of all your upgrade artifacts such as metadata validation results, environment reports, and log files. If you encounter problems during the upgrade, you need to send a copy of this directory to Informatica Global Customer Support for analysis.</td>
</tr>
<tr>
<td>Review the MDM Hub Environment Report</td>
<td>Use the Enterprise Manager tool in the Hub Console to review the current MDM Hub configuration for Hub Servers, Process Servers, the MDM Hub Master Database, and Operational Reference Store databases. Also note the version history of the components. Save a copy of the environment report in the upgrade documentation folder.</td>
</tr>
</tbody>
</table>

Prepare the Environment

Perform the tasks for the upgrade process you chose.
## Clean Upgrade

Perform the following tasks for a clean upgrade:

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verify minimum system requirements | Verify that the machines meet the hardware and software requirements for the MDM Hub installation. The hardware requirements are dependent on the data, processing volumes, and business rules.  
To install the MDM Hub, the machines must meet the following minimum requirements:  
- Disk space. 4.9 GB  
- RAM for the development environment. 4 GB  
To verify the run-time physical memory requirements of the MDM Hub components, use the following formula:  
\[
\text{Total run-time memory requirement for MDM Hub components} = \text{JDK JVM max heap size of the application server} + \text{operating system native heap size}
\] |
| Install Java Development Kit (JDK) | Install a supported version of the JDK on the machine on which you want to install the MDM Hub. The JDK is not bundled with the MDM Hub installers.  
**Note:** Use the same Java version on the application server machines and on the machines on which you want to launch the Hub Console.  
If you want to install Informatica platform on HP-UX, install the supported version of the JDK on the HP-UX machine. The JDK is not bundled with the Informatica platform installer for HP-UX. The JDK is bundled with the Informatica platform installers for all other platforms. |
| Install Visual C++ Redistributable for Visual Studio 2015 on Windows only | On Windows systems, Multidomain MDM requires Visual C++ Redistributable for Visual Studio 2015 to support the name search feature and the matching feature. |
| Set environment variables | Set the environment variables for the MDM Hub installation.  
To use the correct JDK, set the following environment variables to point to the JDK directory:  
- JAVA_HOME. Required  
- PATH. Required  
- INFA_JDK_HOME. Optional. Required if you want to install Informatica platform on AIX or HP-UX.  
To set the correct locale behavior for Oracle, set the NLS_LANG environment variable for client application environments such as the Oracle loader, and the MDM Hub components. Specify the NLS_LANG parameter in the following format:  
\[
\text{NLS_LANG} = \langle \text{language}\rangle_<\text{territory}>._{<\text{character set}>}
\]  
**Note:** To store and search for records that contain Chinese, Japanese, Korean, or accented characters, set the character set to UTF-8.  
For more information about NLS_LANG settings, see the Oracle documentation.  
If you want to install Informatica platform with security enabled for the domain, set the INFA_TRUSTSTORE environment variable to point to the following directory:  
\[
\langle \text{Informatica platform installation directory}\rangle/\text{Client/clients/shared/security}
\] |
| Set the operating system locale | Set the same operating system locale for the Hub Server, the MDM Hub Master Database, Operational Reference Store, and the Hub Console. |
Set up the X Window System on UNIX

If you want to run the installer in graphical mode on UNIX, set up an X Window System. An X Window System is a graphics display server. For more information about setting up an X Window System, see the documentation for your operating system.

Disable access to the root welcome page for your application server

To improve security, disable access to the root welcome page for your application server. For instructions, see the documentation for your application server.

Perform the following additional tasks for a clean upgrade:

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| Validate the metadata       | Ensure the Operational Reference Stores (ORS) do not have any validation errors. If you upgrade the Hub Store when an ORS contains metadata that is not valid, the upgrade might generate unexpected results. Use the Repository Manager in the Hub Console to validate metadata. Resolve any validation issues and then validate the metadata again to confirm that you have resolved the validation issues.  
Save a copy of the final validation results in the `upgradedoc` upgrade documentation folder.  
Use the Repository Manager tool in the MDM Hub Console to validate and then save the validation results. |
| Update persistent ID         | If you use persistent IDs, contact Informatica Global Customer Support. You must update the persistent ID implementation to be compatible with the upgraded version of Multidomain MDM. |

In-place Upgrade

Perform the following tasks for an in-place upgrade:

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| Update the MDM environment to meet system requirements | You might need to update the operating system, application server, JDK, and database server. For system requirements, see the Product Availability Matrix for this version of Multidomain MDM (MDM) on Informatica Network:  
Update the machines that run MDM to be compliant with the current MDM system requirements. |
| Install Visual C++ Redistributable for Visual Studio 2015 on Windows only | On Windows systems, Multidomain MDM requires Visual C++ Redistributable for Visual Studio 2015 to support the name search feature and the matching feature. |
| Validate the metadata       | Ensure the Operational Reference Stores (ORS) do not have any validation errors. If you upgrade the Hub Store when an ORS contains metadata that is not valid, the upgrade might generate unexpected results. Use the Repository Manager in the Hub Console to validate metadata. Resolve any validation issues and then validate the metadata again to confirm that you have resolved the validation issues.  
Save a copy of the final validation results in the `upgradedoc` upgrade documentation folder.  
Use the Repository Manager tool in the MDM Hub Console to validate and then save the validation results. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update persistent ID implementation</strong></td>
<td>If you use persistent IDs, contact Informatica Global Customer Support. You must update the persistent ID implementation to be compatible with the upgraded version of Multidomain MDM.</td>
</tr>
<tr>
<td><strong>Back up the implementation</strong></td>
<td>Back up your current implementation to retain your customizations and allow you to restore the environment. If you encounter issues during the upgrade, you can restore your environment from the backup.</td>
</tr>
<tr>
<td><strong>Back Up the Schema</strong></td>
<td>Perform a full back up of the schema. You cannot roll back schema changes that the upgrade process makes. If you encounter upgrade issues, you can restore the schema from the backup. To back up your schema, see the documentation for the database.</td>
</tr>
<tr>
<td><strong>Back up the Hub Server and Process Server installed directories</strong></td>
<td>Before you install the Hub Server and Process Servers, back up the Hub Server and Process Server installation folders in your environment.</td>
</tr>
<tr>
<td><strong>Back Up Your Data Director Applications</strong></td>
<td>For information about exporting Data Director applications with subject areas, see the <em>Multidomain MDM Data Director Implementation Guide</em>.</td>
</tr>
<tr>
<td><strong>Register or Back Up Customizations</strong></td>
<td>Customizations that you register in the Hub Console such as custom queries, custom functions, and user exits are maintaining during the upgrade process. Back up the latest source code of customizations that you do not register in the Hub Console. Unregistered customizations might be unavailable after you upgrade.</td>
</tr>
<tr>
<td><strong>Back Up Customized Cleanse Engine Configuration Files</strong></td>
<td>Back up any cleanse engine configuration files that you have customized.</td>
</tr>
<tr>
<td><strong>Configure the JAVA_HOME environment variable</strong></td>
<td>JBoss or WebLogic. If you apply the upgrade to the existing installation directory, perform the following steps: 1. In a JBoss environment, manually remove the JAVA_HOME environment variable setting from the following file:  - Windows: <code>&lt;MDM Hub installation directory&gt;\setSiperianEnv.bat</code>  - UNIX: <code>&lt;MDM Hub installation directory&gt;/setSiperianEnv.sh</code> 2. In a JBoss or WebLogic environment, set the JAVA_HOME environment variable to the path of a supported JDK version.</td>
</tr>
<tr>
<td><strong>Disable access to the root welcome page for your application server</strong></td>
<td>To improve security, disable access to the root welcome page for your application server. For instructions, see the documentation for your application server.</td>
</tr>
</tbody>
</table>
Process Existing Jobs

Perform the following tasks to process existing jobs:

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run load job on staging tables that contain records</td>
<td>In Microsoft SQL Server environments, run the load batch job on staging tables that contain records. If you upgrade the Operational Reference Store when the staging tables contain records, the upgrade can fail because the log file size can exceed the available hard drive space.</td>
</tr>
<tr>
<td>Complete stage jobs and delete stage table contents</td>
<td>Before you upgrade the Operational Reference Store, complete any stage jobs that are in progress, and then delete the contents of the stage table. If you do not delete the contents of the stage table, the Operational Reference Store upgrade takes longer than expected to complete in Microsoft SQL Server environments.</td>
</tr>
</tbody>
</table>

Update the MDM Hub Configuration

Perform the following tasks to update the MDM Hub configuration:

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| Grant select right on SYS.V_$PARAMETER for the ORS user | To grant the select right, run the following SQL statement: 
grant select on SYS.V_$PARAMETER to <Operational Reference Store user>;

Remove special characters from names in the subject area configuration | You cannot use special characters in names in the Provisioning tool. If you plan to generate a business entity schema from a subject area configuration, you must first remove any special characters from the names in the subject area configuration.

Ensure column names do not contain reserved words | Additional keywords have been marked as reserved in recent versions of Multidomain MDM. Ensure you do not use reserved keywords in your implementation. For a complete list of reserved words, refer to the "Requirements for Defining Schema Objects" section of the Multidomain MDM Configuration Guide. To request a script that changes the name of a column that contains data, contact Informatica Global Customer Support.

Ensure mapped columns have compatible data types | If you use an Oracle database for your Operational Reference Store, check the mappings from landing table to staging table to ensure that the data types of the mapped columns are compatible. In previous versions, you can create a mapping from a landing table to a staging table where the data types of the mapped columns are not compatible. In this version, the data types of the mapped columns must be compatible. When you load data, if there is a data type mismatch, the load fails with an error in the log files. For more information about mapping columns, see the Multidomain MDM Configuration Guide. |
Upgrade Task | Details
--- | ---
Back up your user preferences from the C_REPOS_DS_PREF table and the C_REPOS_DS_PREF_DETAIL table | If your Data Director environment includes user preferences for shown or hidden columns, the settings are lost when you upgrade because the cryptographic hash algorithm has changed in this version. After you upgrade, recreate your user preferences. For more information about Data Director global properties, see the Multidomain MDM Data Director Implementation Guide.
Ensure users have a valid email address | Ensure that existing users have valid email addresses associated with their user names in the Hub Console. To reset their passwords to access the MDM Hub, users must have a valid email address. For more information about editing user information in the Hub Console, see the Multidomain MDM Security Guide. Note: You cannot change the email address for the admin user in the Hub Console. To change the email address for the admin user, update the admin user entry directly in the C_REPOS_USER table under CMX_SYSTEM schema.
Register indexes | If you upgrade schemas with custom indexes, you must register the custom indexes. Use the RegisterCustomIndex SIF API to register the custom indexes. For more information about the RegisterCustomIndex SIF API, see the Multidomain MDM Services Integration Framework Guide.

Register the Operational Reference Stores with the Original Schema Owner

If any of the Operational Reference Store (ORS) databases are registered with a proxy user, register the ORS database with the original schema owner. You must register the ORS with the original schema owner to ensure that you have sufficient privileges to perform the upgrade operations. You can reregister the ORS with the proxy user after you upgrade. The original default schema owner is CMX_ORS.

1. Start the Hub Console.
   The Change database dialog box appears.
2. Select the MDM Hub Master database, and click Connect.
3. Select the Databases tool from the Configuration workbench.
4. Select Write Lock > Acquire Lock.
5. Click the Register database button.
   The Informatica MDM Hub Connection Wizard appears and prompts you to select the database type.
6. Select the type of database, and click Next.
7. Configure connection properties for the database.
   a. Select an Oracle connection method, and then click **Next**.
      You can select the following Oracle connection methods:
      - **Service**
        Connect to Oracle by using the service name.
      - **SID**
        Connect to Oracle by using the Oracle System ID.
      For more information about SERVICE and SID names, see the Oracle documentation.
      The **Connection Properties** page appears.
   b. Specify the connection properties for the connection type that you select, and click **Next**.
      You can configure the following connection properties:
      - **Database Display Name**
        Name for the Operational Reference Store that must appear in the Hub Console.
      - **Machine Identifier**
        Prefix given to keys to uniquely identify records from the Hub Store instance.
      - **Database host name**
        IP address or name of the server that hosts the Oracle database.
      - **SID**
        Oracle System Identifier that refers to the instance of the Oracle database running on the server. The **SID** field appears if you selected the **SID** connection type.
      - **Service**
        Name of the Oracle SERVICE used to connect to the Oracle database. The **Service** field appears if you selected the **Service** connection type.
      - **Port**
        The TCP port of the Oracle listener running on the Oracle database server. The default is 1521.
      - **Oracle TNS Name**
        Name by which the database is known on your network as defined in the `TNSNAMES.ORA` file of the application server.
        For example: `mydatabase.mycompany.com`.
        You set the Oracle TNS name when you install the Oracle database. For more information about the Oracle TNS name, see the Oracle documentation.
      - **Schema Name**
        Name of the Operational Reference Store.
      - **User name**
        Specify the original user name for the ORS. Default is CMX_ORS.
      - **Password**
        Password associated with the original user for the ORS.
      The **Summary** page appears.
c. Review the summary, and specify additional connection properties.

The following table describes the additional connection properties that you can configure:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection URL</td>
<td>Connect URL. The Connection Wizard generates the connect URL by default. The following list shows the format of the connect URL for the Oracle connection types: Service connection type: jdbc:oracle:thin:@database_host:port/service_name SID connection type: jdbc:oracle:thin:@database_host:port:sid For a service connection type, you have the option to customize and later test a different connection URL.</td>
</tr>
<tr>
<td>Create datasource after registration</td>
<td>Select to create the datasource on the application server after registration. <strong>Note:</strong> If you do not select the option, you must manually configure the data source.</td>
</tr>
</tbody>
</table>

d. For a service connection type, if you want to change the default URL, click the **Edit** button, specify the URL, and then click **OK**.

8. Click **Finish**.

The **Registering Database** dialog box appears.

9. Click **OK**.

The MDM Hub registers the ORS.

---

### Prepare the BPM Upgrade

Perform the following tasks to prepare for the BPM upgrade:
Choose a workflow adapter

Review the following upgrade options for workflow adapters, and choose the upgrade option that suits your needs:

<table>
<thead>
<tr>
<th>Current Workflow Adapter</th>
<th>Upgrade Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIPERIAN</td>
<td>Deprecated.</td>
</tr>
<tr>
<td></td>
<td><strong>Option 1</strong></td>
</tr>
<tr>
<td></td>
<td>Keep SIPERIAN as the primary workflow adapter.</td>
</tr>
<tr>
<td></td>
<td><strong>Option 2</strong></td>
</tr>
<tr>
<td></td>
<td>Upgrade to the BE ActiveVOS workflow adapter based on business entities. You must have a business entity configuration to use the BE ActiveVOS workflow adapter.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <em>Migrating IDD Applications to the Business Entity Data Model</em>.</td>
</tr>
<tr>
<td>Informatica ActiveVOS</td>
<td>This workflow adapter is based on subject areas and operates using SIF APIs.</td>
</tr>
<tr>
<td></td>
<td><strong>Option 1</strong></td>
</tr>
<tr>
<td></td>
<td>Keep Informatica ActiveVOS as the primary workflow adapter.</td>
</tr>
<tr>
<td></td>
<td><strong>Option 2</strong></td>
</tr>
<tr>
<td></td>
<td>Upgrade to the BE ActiveVOS workflow adapter based on business entities. You must have a business entity configuration to use the BE ActiveVOS workflow adapter.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>Multidomain MDM Data Director Migration Guide</em>.</td>
</tr>
<tr>
<td>BE ActiveVOS</td>
<td>This workflow adapter is based on business entities and operates using business entity services. You must use the version of ActiveVOS that is defined in the Product Availability Matrix. If an older version is detected in your environment, the upgrade process installs the required version of ActiveVOS.</td>
</tr>
</tbody>
</table>

Prepare to move from standalone ActiveVOS to embedded ActiveVOS (In-place Upgrade)

If you are upgrading existing machines and want to move from standalone ActiveVOS to embedded ActiveVOS, perform the following upgrade tasks:

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove the ActiveVOS data sources</td>
<td>If the standalone ActiveVOS server is in the same JBoss instance, WebSphere profile, or WebLogic domain as Multidomain MDM, remove the data source for ActiveVOS from the application server.</td>
</tr>
</tbody>
</table>
| Edit the URN mapping in a WebSphere environment    | 1. Launch the ActiveVOS Console. In a browser, type the following URL, substituting the correct host name and port number:  
  - Secure connections: https://<host>:<port>/activevos  
  - Non-secure connections: http://<host>:<port>/activevos  
  2. In the ActiveVOS Console, on the Home page, click Administration > Configure Server > URN Mappings.  
  3. Ensure that URN java:comp/env/jdbc/ActiveVOS maps to URL java:comp/env/jdbc/ActiveVOS.                                                                                                           |
Edit the build.properties file (In-place Upgrade)

If you use ActiveVOS, perform the following tasks to edit the build.properties file:

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
</table>
| Configure the database connection properties for IBM DB2 | In IBM DB2 environments, before you upgrade, add the ActiveVOS database connection properties to the build.properties file in &lt;MDM Hub installation directory&gt;/hub/server/bin.  
The following sample shows the ActiveVOS database connection properties with sample entries:  
activevos.db.type=db2  
activevos.db.server=localhost  
activevos.db.port=50000  
activevos.db.user=AVOS  
activevos.db.dbname=INFA102  
activevos.db.schemaname=AVOS  
activevos.db.jdbc.url=jdbc:db2://localhost:50000/INFA102  
| Configure the ActiveVOS installation directory   | If the upgrade process detects that the installed version of ActiveVOS does not meet the system requirements, the upgrade process installs the required version of ActiveVOS in a new directory.  
To install ActiveVOS in the same directory as a previous installation, delete or comment out the following entry in the build.properties file:  
activevosinstall.dir=&lt;ActiveVOS installation directory&gt; |
Database Tasks

This chapter includes the following topics:

- Database Tasks Overview, 26
- Set Up Oracle Database, 26
- Set Up Microsoft SQL Server, 32
- Set Up IBM DB2 Database, 36

Database Tasks Overview

Configure your database to work with Multidomain MDM. Follow the instructions for your database.

When you perform a clean upgrade, perform all the steps for your database as you would for a new installation of Multidomain MDM.

When you perform an in-place upgrade where your database version is still supported, verify that the database is configured to work with this version of Multidomain MDM.

Set Up Oracle Database

Before you create an MDM Hub Master Database and Operational Reference Store, set up the database environment.

To set up the database environment, perform the following tasks:

1. Install and configure Oracle.
2. Set up a database instance.
3. Set up database privileges and connections.
4. Create the ActiveVOS schema.
Step 1. Install and Configure Oracle

You can install and configure Oracle Database according to the instructions in the Oracle documentation.

The following table describes the Oracle installation and configuration tasks:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Oracle</td>
<td>Install the supported version of Oracle Database. Note: If you want to use the Oracle multitenant feature, set up a pluggable database (PDB) for the MDM Hub installation.</td>
</tr>
<tr>
<td>Install clients and utilities</td>
<td>Install the Oracle client and utilities software to communicate with the MDM Hub, and to run the MDM Hub processes. On each machine where you want to run the Hub Server or Process Server, install the following software: · Oracle client · SQL*Loader</td>
</tr>
<tr>
<td>Disable recycle bins</td>
<td>Disable the recycle bins, USER_RECYCLEBIN and DBA_RECYCLEBIN. Recycle bins can interfere with the MDM Hub processes. Disable the recycle bins at the system or session level. Also, purge existing objects in the recycle bin.</td>
</tr>
<tr>
<td>Set initialization parameters</td>
<td>Configure the Oracle initialization parameters in the init.ora file. For information about Oracle initialization parameters, see the MDM Multidomain Edition Performance Tuning Guide.</td>
</tr>
</tbody>
</table>

For information about installing and configuring Oracle, see the Oracle documentation.

Step 2. Set Up Database Instances

After you install and configure Oracle Database, create and set up database instances.

The following table describes the tasks that you need to perform to set up a database instance:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a database instance</td>
<td>Create a database instance. For an MDM Hub with multiple Operational Reference Stores distributed across different host machines, create a database instance on each host machine.</td>
</tr>
<tr>
<td>Create tablespaces</td>
<td>Create tablespaces for the MDM Hub data. Adjust the default tablespace sizes and the number of data files based on the volume of data that you want to load into the MDM Hub. Create the following tablespaces: · CMX_DATA. Contains the metadata and user data of the MDM Hub. · CMX_INDEX. Contains indexes that the MDM Hub creates and uses. · CMX_TEMP. Contains temporary tables for Informatica MDM Hub.</td>
</tr>
</tbody>
</table>
Creating Tablespaces on Premises

If you use Oracle on premises, create tablespaces as permanent tablespaces that you manage locally or configure manually.

**Note:** Create bigfile tablespaces to simplify database management for large data loads. However, you can create smallfile tablespaces if required.

1. Log in to Oracle as a database administrative user such as SYSTEM.
2. Create the tablespaces.

The following table contains sample SQL statements to create tablespaces:

<table>
<thead>
<tr>
<th>Default Tablespace Name</th>
<th>Sample SQL Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMX_DATA</td>
<td>CREATE BIGFILE TABLESPACE CMX_DATA NOLOGGING DATAFILE '&lt;Oracle install directory&gt;/CMX_DATA1.dbf' SIZE 2048M REUSE EXTENT MANAGEMENT LOCAL; Do not change the default tablespace name to prevent Repository Manager validation errors.</td>
</tr>
<tr>
<td>CMX_INDEX</td>
<td>CREATE BIGFILE TABLESPACE CMX_INDEX NOLOGGING DATAFILE '&lt;Oracle install directory&gt;/CMX_INDEX1.dbf' SIZE 2048M REUSE EXTENT MANAGEMENT LOCAL;</td>
</tr>
<tr>
<td>CMX_TEMP</td>
<td>CREATE BIGFILE TABLESPACE CMX_TEMP NOLOGGING DATAFILE '&lt;Oracle install directory&gt;/CMX_TEMP1.dbf' SIZE 2048M REUSE EXTENT MANAGEMENT LOCAL;</td>
</tr>
</tbody>
</table>

Creating Tablespaces in Amazon Relational Database Service

If you use Amazon Relational Database Service (RDS) for Oracle, create tablespaces as permanent tablespaces in Amazon RDS.

**Note:** Create bigfile tablespaces to simplify database management for large data loads. However, you can create smallfile tablespaces if required.

1. Log in to Amazon RDS for Oracle as a database administrative user.
2. Create the tablespaces.
The following table contains sample SQL statements to create tablespaces:

<table>
<thead>
<tr>
<th>Default Tablespace Name</th>
<th>Sample SQL Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMX_DATA</td>
<td>CREATE BIGFILE TABLESPACE CMX_DATA        DATAFILE SIZE 2048M AUTOEXTEND ON NEXT 2048M;</td>
</tr>
<tr>
<td></td>
<td>Do not change the default tablespace name to prevent Repository Manager validation errors.</td>
</tr>
<tr>
<td>CMX_INDEX</td>
<td>CREATE BIGFILE TABLESPACE CMX_INDEX     DATAFILE SIZE 2048M AUTOEXTEND ON NEXT 2048M;</td>
</tr>
<tr>
<td>CMX_TEMP</td>
<td>CREATE BIGFILE TABLESPACE CMX_TEMP     DATAFILE SIZE 2048M AUTOEXTEND ON NEXT 2048M;</td>
</tr>
</tbody>
</table>

Configuring the Database Environment for Custom Tablespace Names

If you use a tablespace name other than the default tablespace name for CMX_INDEX or CMX_TEMP, disable the DEFERRED_SEGMENT_CREATION initialization parameter. You disable the parameter to prevent Repository Manager validation errors.

- To disable DEFERRED_SEGMENT_CREATION, run the following SQL statement, and restart the database:
  
  ```sql
  ALTER SYSTEM SET DEFERRED_SEGMENT_CREATION=false SCOPE=BOTH;
  ```
Step 3. Set Up Database Privileges and Connections

Set up database privileges and connections.

The following table describes the tasks that you need to perform to set up database privileges and connections:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grant privileges to the database administrative user</td>
<td>If you want to use a database administrative user to create the MDM Hub Master Database and the Operational Reference Store, grant privileges to the database administrative user. The user must have the privileges to grant options for distributed transactions and <code>DBMS_LOCK</code>. To grant privileges to the database administrative user, connect to the database as a user with privileges to grant options, and run the following SQL statements: <code>GRANT SELECT ON sys.pending_trans$ TO &lt;DBA user&gt; with grant option;</code>, <code>GRANT SELECT ON sys.dba_pending_transactions TO &lt;DBA user&gt; with grant option;</code>, <code>GRANT SELECT ON sys.dba_2pc_pending TO &lt;DBA user&gt; with grant option;</code>, <code>GRANT EXECUTE ON sys.dbs_xa TO &lt;DBA user&gt; with grant option;</code>, <code>GRANT EXECUTE ON sys.dbs_lock TO &lt;DBA user&gt; with grant option;</code></td>
</tr>
</tbody>
</table>
| Add the Oracle TNS name                     | For connections to the Oracle database, add TNS name entries to the `tnsnames.ora` file on the Hub Server and Process Server machines. To add TNS name entries, use the following syntax: `<TNS NAME> =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <Oracle server host name>))
      (PORT = <Oracle server port>))
    )
  )
  (CONNECT_DATA =
    (SERVICE_NAME = <Oracle SID>)
  )
)                                                                                                                                                                                                 |
| Test the database connection                | Test the connection to the database from each machine on which you want to run the Hub Server or the Process Server. In SQL*Plus, use the following SQL statement syntax: `sqlplus <user name>/<password>@<TNS Name>`                                                                 |

Step 4. Create the ActiveVOS Schema

If you want to install ActiveVOS, you need to create the ActiveVOS database schema. To create the schema, run the `create_bpm` script.

1. Open a command prompt and change to the following directory: `<MDM Hub distribution directory>/database/bin`
2. Run the following command:
   - On UNIX: `./sip_ant.sh create_bpm`
   - On Windows: `sip_ant.bat create_bpm`
3. Answer the prompts that appear.
The prompt displays default text in brackets. Press **Enter** to use the default value and go to the next prompt.

**Note:** IBM DB2 data sources are case-sensitive. To avoid issues related to case-sensitivity, Informatica recommends that you use uppercase letters to define names, such as those for schemas, columns, and triggers.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database to use. For IBM DB2, specify DB2. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database TCP/IP Port</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td>ActiveVOS Database Name</td>
<td>Name of the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Schema/User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the database administrative user.</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS Tablespace Name</td>
<td>The name of the tablespace that contains the records that are involved in MDM workflows.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>The type of database. For an Oracle database, specify Oracle. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
</tbody>
</table>
| Oracle Connection Type            | Connection type. Use one of the following values:  
  - SERVICE. Uses the service name to connect to Oracle.  
  - SID. Uses the Oracle System ID to connect to Oracle.                                                                                                                                                     |
| ActiveVOS Database Host Name      | Name of the machine that hosts the database.                                                                                                                                                                 |
| ActiveVOS Database Port           | Port number that the database listener uses.                                                                                                                                                                  |
| Database Service Name             | Name of the Oracle service. This property is required when the selected Oracle connection type is SERVICE.                                                                                                  |
| Oracle Net Connect Identifier (TNS Name) | Oracle TNS name.                                                                                                                                                                                          |
| Database SID                      | Name of the Oracle System ID. This property is required when the selected Oracle connection type is SID.                                                                                                   |
### Property | Description
--- | ---
**DBA User Name** | User name of the database administrative user.
**DBA Password** | Password of the administrative user.
**ActiveVOS User Name** | User name of the ActiveVOS Server administrative user.
**ActiveVOS User Password** | Password of the administrative user.
**ActiveVOS User Tablespace** | The name of the tablespace that contains the records that are involved in MDM workflows.
**ActiveVOS User Temp Tablespace** | The name of the temporary tablespace.

### Property | Description
--- | ---
**Database Type** | Type of database to use. For Microsoft SQL Server, specify MSSQL. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.
**ActiveVOS User Name** | User name of the ActiveVOS Server administrative user.
**ActiveVOS User Password** | Password of the administrative user.
**ActiveVOS Collation Name** | Name of the ActiveVOS database collation. For example, Latin1_General_CI_AS.
**ActiveVOS Database Host Name** | Name of the machine that hosts the database.
**ActiveVOS Database Path** | Path to the database location.
**DBA User Name** | User name of the SA user.
**DBA Password** | Password of the SA user account.

4. After you create the schema, review the *sip_ant.log* file in the following directory:

   `<MDM Hub distribution directory>/database/bin`

   The *sip_ant.log* file logs any errors that might occur when you run the *sip_ant* script to create the ActiveVOS database schema.

---

### Set Up Microsoft SQL Server

Before you create an MDM Hub Master Database and Operational Reference Store, set up the database environment.

To set up the database environment, perform the following tasks:

1. Install and configure Microsoft SQL Server.
2. Create a data file store.
3. Install ODBC driver.
4. Create the ActiveVOS schema.

Step 1. Install and Configure Microsoft SQL Server

You can install and configure Microsoft SQL Server according to the instructions in the Microsoft SQL Server documentation.

The following table describes the Microsoft SQL Server installation and configuration tasks:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Microsoft SQL Server</td>
<td>Install the supported version of Microsoft SQL Server. <strong>Note:</strong> Ensure that you specify mixed mode as the database engine authentication security mode.</td>
</tr>
<tr>
<td>Configure distributed transactions</td>
<td>Configure Microsoft SQL Server for distributed transactions because the MDM Hub requires a distributed transactions environment. To configure Microsoft SQL Server for distributed transactions, enable MS DTC for XA transactions, and configure the JDBC distributed transactions component.</td>
</tr>
<tr>
<td>Enable the TCP/IP network protocol</td>
<td>Configure Microsoft SQL Server to use the TCP/IP network protocol that the MDM Hub environment requires.</td>
</tr>
</tbody>
</table>

Configuring Microsoft SQL Server for Distributed Transactions

Before you start Microsoft SQL Server, ensure that you configure it for distributed transactions. The MDM Hub requires a distributed transaction environment.

1. To ensure that the Microsoft Distributed Transaction Coordinator (MS DTC) service starts when you start Microsoft SQL Server, mark MS DTC as Automatic in the Service Manager.
2. Enable MS DTC for XA transactions.
3. Enable MS DTC for SNA LU 6.2 transactions.
4. Configure the JDBC distributed transactions component.
   a. Download and extract the Microsoft SQL Server JDBC driver from the Microsoft website to a directory on the machine.
   b. Copy the sqljdbc_xa.dll file to the Bin directory of the machine on which Microsoft SQL Server is installed.
   c. Run the xa_install.sql script on the Microsoft SQL Server instance as an administrator. The xa_install.sql script is in the xa directory of the JDBC driver.
   d. Verify that the script creates the SqlJDBCXAUser role in the Microsoft SQL Server master database.

For more information about how to install and configure Microsoft SQL Server for distributed transactions, see the Microsoft SQL Server documentation.
Enabling the TCP/IP Network Protocol

Use SQL Server Configuration Manager to enable the TCP/IP network protocol, which the MDM Hub environment requires.

1. Start the SQL Server Configuration Manager.
2. In the console pane, expand SQL Server Network Configuration, and then click Protocols for MSSQLSERVER.
3. In the details pane, right-click TCP/IP, and then click Enable.
4. Restart the SQL Server service.

The TCP/IP network protocol is enabled.

Step 2. Create a Microsoft SQL Server Data File Store

Ensure that you create a Microsoft SQL Server data file store if one does not exist. When you create the MDM Hub Master Database and the Operational Reference Stores, you need to provide the path to the Microsoft SQL Server data file store.

Step 3. Install ODBC Driver

If you install the application server on UNIX or Linux, install an ODBC driver for Microsoft SQL Server so that data sources can be created.

- Download and install the ODBC driver for the operating system.
  - On Linux. Download the Microsoft SQL Server ODBC driver from the Microsoft website.
  - On UNIX. Download the UNIX ODBC driver from the unixODBC Project home page.

Step 4. Create the ActiveVOS Schema

If you want to install ActiveVOS, you need to create the ActiveVOS database schema. To create the schema, run the create_bpm script.

1. Open a command prompt and change to the following directory:
   
   `<MDM Hub distribution directory>/database/bin`

2. Run the following command:
   
   On UNIX. `./sip_ant.sh create_bpm`
   
   On Windows. `sip_ant.bat create_bpm`

3. Answer the prompts that appear.
   
   The prompt displays default text in brackets. Press Enter to use the default value and go to the next prompt.
Note: IBM DB2 data sources are case-sensitive. To avoid issues related to case-sensitivity, Informatica recommends that you use uppercase letters to define names, such as those for schemas, columns, and triggers.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database to use. For IBM DB2, specify <strong>DB2</strong>. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database TCP/IP Port</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td>ActiveVOS Database Name</td>
<td>Name of the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Schema/User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the database administrative user.</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS Tablespace Name</td>
<td>The name of the tablespace that contains the records that are involved in MDM workflows.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>The type of database. For an Oracle database, specify <strong>Oracle</strong>. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>Oracle Connection Type</td>
<td>Connection type. Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td>- SERVICE. Uses the service name to connect to Oracle.</td>
</tr>
<tr>
<td></td>
<td>- SID. Uses the Oracle System ID to connect to Oracle.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Port</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td>Database Service Name</td>
<td>Name of the Oracle service. This property is required when the selected Oracle connection type is SERVICE.</td>
</tr>
<tr>
<td>Oracle Net Connect Identifier (TNS Name)</td>
<td>Oracle TNS name.</td>
</tr>
<tr>
<td>Database SID</td>
<td>Name of the Oracle System ID. This property is required when the selected Oracle connection type is SID.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the database administrative user.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Tablespace</td>
<td>The name of the tablespace that contains the records that are involved in MDM workflows.</td>
</tr>
<tr>
<td>ActiveVOS User Temp Tablespace</td>
<td>The name of the temporary tablespace.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database to use. For Microsoft SQL Server, specify MSSQL. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>ActiveVOS User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS Collation Name</td>
<td>Name of the ActiveVOS database collation. For example, Latin1_General_CI_AS.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Path</td>
<td>Path to the database location.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the SA user.</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the SA user account.</td>
</tr>
</tbody>
</table>

4. After you create the schema, review the `sip_ant.log` file in the following directory:

   `<MDM Hub distribution directory>/database/bin`

   The `sip_ant.log` file logs any errors that might occur when you run the `sip_ant` script to create the ActiveVOS database schema.

---

**Set Up IBM DB2 Database**

Before you create an MDM Hub Master Database and Operational Reference Store, set up the database environment.

To set up the database environment, perform the following tasks:

1. Install and configure IBM DB2.
2. Create a database and tablespace.
4. Create the ActiveVOS schema.

**Step 1. Install and Configure IBM DB2**

You can install and configure IBM DB2 according to the instructions in the IBM DB2 documentation.

The following table describes the IBM DB2 installation and configuration tasks:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install IBM DB2</td>
<td>Install the supported version of IBM DB2.</td>
</tr>
</tbody>
</table>
| Install clients and utilities | Install the IBM DB2 client and utilities software to communicate with the MDM Hub and run the MDM Hub processes. On each machine where you want to run the Hub Server or Process Server, install the following software:  
  - DB2 client  
  - DB2 Java utilities for the DB2 client  
  Ensure that you catalog the IBM DB2 database from each DB2 client. |
| Configure IBM DB2 drivers     | To configure IBM DB2 drivers, copy the db2jcc.jar and db2jcc_license_cu.jar driver files from the source to the target directory:  
  Source: <IBM DB2 installation directory>/java  
  Target: <MDM Hub distribution directory>/database/lib |
| Create the MDM Hub schema users | Create users to access the following MDM Hub schemas:  
  - MDM Hub Master Databases  
  - Operational Reference Stores |

**Step 2. Create a Database and Tablespaces**

After you install and configure IBM DB2, create and configure a database and tablespaces.

The following table describes the tablespaces that you require for the MDM Hub schemas:

<table>
<thead>
<tr>
<th>Tablespace Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMX_DATA</td>
<td>Default tablespace for the Operational Reference Store schema. Contains the metadata and user data of the MDM Hub.</td>
</tr>
<tr>
<td>CMX_INDX</td>
<td>Tablespace to contain indexes that the MDM Hub creates and uses.</td>
</tr>
<tr>
<td>CMX_TEMP</td>
<td>Tablespace to contain temporary tables that the MDM Hub creates and uses.</td>
</tr>
<tr>
<td>CMX_REPOS</td>
<td>Tablespace to contain the Operational Reference Store objects.</td>
</tr>
<tr>
<td>CMX_USER_TEMP</td>
<td>Temporary tablespace to contain operational temporary tables.</td>
</tr>
<tr>
<td>CMX_SYS_TEMP</td>
<td>Temporary tablespace for SQL operations.</td>
</tr>
</tbody>
</table>

Use one of the following procedures to create a database and tablespaces:

- Manually create the database and tablespaces
• Use a script to create the database and tablespaces

**Manually Create a Database and Tablespaces**

You can manually create a database and tablespaces. Ensure that you create the database with the compatibility vector turned on and with the `UTF-8 TERRITORY US` locale.

Set the DB2 Environment and DB2 Registry Variables

If you create the database manually, set the DB2 environment and DB2 registry variables that the MDM Hub requires.

Use the following commands to set the DB2 environment and DB2 registry variables:

```plaintext
db2set DB2CODEPAGE=1208
db2set DB2_COMPATIBILITY VECTOR=
db2set DB2_DEFERRED_PREPARE SEMANTICS=YES
db2set DB2_RESTORE_GRANTED ADMINAuthorities=ON
db2set DB2_HASH JOIN=YES
db2set DB2_ANTJOIN=YES
db2set DB2_INLIST_TO_NILJN=NO
db2set DB2_SELECTIVITY=ALL
db2set DB2_SKIPINSERTED=YES
db2set DB2_SKIPDELETED=YES
db2set DB2_EXTENDED_OPTIMIZATION=ON,ENHANCED_MULTIPLE_DISTINCT,IXOR,SNHD
db2set DB2NTOCACHE=ON
db2set DB2_REDUCED_OPTIMIZATION=REDUCE_LOCKING
```

Set the Database Manager Configuration for the Database Instance

You need to optimize the database manager configuration for the database instance.

Use the following commands to optimize the database manager configuration:

```plaintext
db2 update dbm cfg using MON_HEAP_SZ AUTOMATIC
db2 update dbm cfg using JAVA_HEAP_SZ 2048
db2 update dbm cfg using AGENT_STACK_SZ 256
db2 update dbm cfg using SHEAPTHRES 0
db2 update dbm cfg using INTRA_PARALLEL YES
```

**Note:** The values specified in the commands are minimum requirements for the MDM Hub.

Set Database Configuration Parameters

Set the configuration parameters for the database.

Use the following commands to set the database configuration parameters:

```plaintext
db2 update db cfg using LOCKLIST AUTOMATIC
db2 update db cfg using MAXLOCKS AUTOMATIC
db2 update db cfg using PCKCACHESZ 128000
db2 update db cfg using DBHEAP AUTOMATIC
db2 update db cfg using CATALOGCACHE_SZ 25000
db2 update db cfg using LOGBUFFSZ 4096
db2 update db cfg using UTIL_HEAP_SZ 50000
db2 update db cfg using BUFFPAGE 250
db2 update db cfg using STM_HEAP AUTOMATIC
db2 update db cfg using APPLHEAPSZ AUTOMATIC
db2 update db cfg using APPL_MEMORY AUTOMATIC
db2 update db cfg using STAT_HEAP_SZ AUTOMATIC
db2 update db cfg using LOGFLSIZ 128000
db2 update db cfg using LOGPRIMARY 10
db2 update db cfg using LOGSECOND 200
db2 update db cfg using auto_reval deferred_force
db2 update db cfg using decflt_rounding round_half_up
db2 update db cfg using SHEAPTHRES SHR AUTOMATIC
db2 update db cfg using DFT DEGREE 1
```

**Note:** The values specified in the commands are minimum requirements for the MDM Hub.
Grant Privileges to SYSIBMADM Modules

You must grant privileges to UTL_DIR, UTL_FILE, and DBMS_SQL SYSIBMADM modules.

Use the following commands to grant privileges to modules:

```sql
GRANT EXECUTE ON MODULE SYSIBMADM.UTL_DIR TO PUBLIC WITH GRANT OPTION
GRANT EXECUTE ON MODULE SYSIBMADM.UTL_FILE TO PUBLIC WITH GRANT OPTION
GRANT EXECUTE ON MODULE SYSIBMADM.DBMS_SQL TO PUBLIC WITH GRANT OPTION
```

Define Buffer Pools for the Database Manager

Define the REPOS_POOL and CMX_POOL buffer pools.

Use the following commands to define buffer pools:

```sql
CREATE BUFFERPOOL REPOS_POOL IMMEDIATE SIZE 1500 PAGESIZE 32 K
CREATE BUFFERPOOL CMX_POOL IMMEDIATE SIZE 3000 PAGESIZE 32 K
```

Create Tablespace

You need to create tablespaces that the MDM Hub schemas require.

Create the tablespaces in the following sequence:

1. CMX_DATA
2. CMX_INDEX
3. CMX_REPOS
4. CMX_TEMP
5. CMX_USER_TEMP
6. CMX_SYS_TEMP

Use the following statements to create tablespaces for the MDM Hub schemas:

```sql
CREATE TABLESPACE CMX_DATA PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'c:\dbhub9x\CMX_DATA\cmx_data01.dat' 500 M )
EXTENTSIZE 16
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL CMX_POOL

CREATE TABLESPACE CMX_INDEX PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'c:\dbhub9x\CMX_INDEX\cmx_index01.dat' 500 M )
EXTENTSIZE 16
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL CMX_POOL

CREATE TABLESPACE CMX_REPOS PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'c:\dbhub9x\CMX_REPOS\cmx_repos01.dat' 500 M )
EXTENTSIZE 16
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL REPOS_POOL

CREATE TABLESPACE CMX_TEMP PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'c:\dbhub9x\CMX_TEMP\cmx_temp01.dat' 500 M )
EXTENTSIZE 16
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL CMX_POOL

CREATE USER TEMPORARY TABLESPACE CMX_USER_TEMP PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'c:\dbhub9x\USER_TEMP\cmx_user_temp01.dat' 500 M )
EXTENTSIZE 16
```

Set Up IBM DB2 Database 39
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL CMX_POOL

CREATE SYSTEM TEMPORARY TABLESPACE CMX_SYS_TEMP PAGESIZE 32 K
MANAGED BY DATABASE USING ( FILE 'C:\d\hub9x\SYSTEM_TEMP\cmx_sys_temp01.dat' 500 M )
EXTENTSIZE 16
AUTORESIZE YES
OVERHEAD 10.5
PREFETCHSIZE 16
BUFFERPOOL CMX_POOL

Optionally, to create tablespaces with the dropped table recovery feature enabled, add the following clause to
the CREATE TABLESPACE statement:
DROPPED TABLE RECOVERY ON

Use a Script to Create a Database and Tablespaces

The MDM Hub distribution includes a script to create the database and associated tablespaces. To run the
script, you need administrative privileges with write and execute permissions to the DB2 data directory.

On UNIX, before you create the database, update the `db2.storage.path` property in the
database.properties file with the correct database storage path. The database.properties file is in the
following directory:

<MDM Hub distribution directory>/database/bin/db2

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

   <MDM Hub distribution directory>/database/bin

2. To create the database, run the following command:

   On UNIX, ./sip_ant.sh create_db
   On Windows, sip_ant.bat create_db

3. Answer the prompts described in the following table:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the database type (ORACLE, MSSQL, DB2)</td>
<td>Database type. Specify DB2.</td>
</tr>
<tr>
<td>Enter the database instance name [db2]</td>
<td>Name of the database instance. Default is db2.</td>
</tr>
<tr>
<td>Enter the database name [SIP97]</td>
<td>Name of the database. Default is SIP97.</td>
</tr>
<tr>
<td>Enter the database storage path [C: \DB2DATA]</td>
<td>Path to the directory where the database must be stored. Default is C: \DB2DATA.</td>
</tr>
<tr>
<td><strong>Note:</strong> On UNIX, accept the default value. The database storage path that you specify in the database.properties file will be used.</td>
<td></td>
</tr>
<tr>
<td>Prompt</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Enter the DBA user name [DB2ADMIN]</td>
<td>User name of the administrative user. Default is DB2ADMIN.</td>
</tr>
<tr>
<td>Enter the DBA password</td>
<td>Password of the administrative user.</td>
</tr>
</tbody>
</table>

The script creates the database and the following tablespaces:

- CMX_DATA
- CMX_INDX
- CMX_TEMP
- CMX_REPOS
- CMX_USER_TEMP
- CMX_SYS_TEMP

To verify that the database was created successfully, review the `sip_ant.log` file in the `<MDM Hub distribution directory>/database/bin` directory.

### Step 3. Bind Packages on the Database Server

To ensure that the IBM DB2 client can connect to the database server to run DB2 commands, bind packages on the database server.

1. Open an IBM DB2 command window, and change to the following directory:
   `<IBM DB2 installation directory>/SQLLIB/bnd`
2. Connect to the database by running the following command:
   ```
   db2 connect to <database name> user <database user> using <database user password>
   ```
   **Note:** The database user must have the bind permission.
3. Run the following bind command:
   ```
   db2 bind @db2cli.lst blocking all grant public sqlerror continue CLIPKG 10
   ```
   The required packages are bound to the database server.

### Step 4. Create the ActiveVOS Schema

If you want to install ActiveVOS, you need to create the ActiveVOS database schema. To create the schema, run the `create_bpm` script.

1. Open a command prompt and change to the following directory:
   `<MDM Hub distribution directory>/database/bin`
2. Run the following command:
   - On UNIX: `./sip_ant.sh create_bpm`
   - On Windows: `sip_ant.bat create_bpm`
3. Answer the prompts that appear.
   The prompt displays default text in brackets. Press **Enter** to use the default value and go to the next prompt.
**Note:** IBM DB2 data sources are case-sensitive. To avoid issues related to case-sensitivity, Informatica recommends that you use uppercase letters to define names, such as those for schemas, columns, and triggers.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database to use. For IBM DB2, specify <strong>DB2</strong>. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database TCP/IP Port</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td>ActiveVOS Database Name</td>
<td>Name of the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Schema/User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the database administrative user.</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS Tablespace Name</td>
<td>The name of the tablespace that contains the records that are involved in MDM workflows.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>The type of database. For an Oracle database, specify <strong>Oracle</strong>. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>Oracle Connection Type</td>
<td>Connection type. Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td>- SERVICE. Uses the service name to connect to Oracle.</td>
</tr>
<tr>
<td></td>
<td>- SID. Uses the Oracle System ID to connect to Oracle.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Port</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td>Database Service Name</td>
<td>Name of the Oracle service. This property is required when the selected Oracle connection type is SERVICE.</td>
</tr>
<tr>
<td>Oracle Net Connect Identifier (TNS Name)</td>
<td>Oracle TNS name.</td>
</tr>
<tr>
<td>Database SID</td>
<td>Name of the Oracle System ID. This property is required when the selected Oracle connection type is SID.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the database administrative user.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Tablespace</td>
<td>The name of the tablespace that contains the records that are involved in MDM workflows.</td>
</tr>
<tr>
<td>ActiveVOS User Temp Tablespace</td>
<td>The name of the temporary tablespace.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Type</td>
<td>Type of database to use. For Microsoft SQL Server, specify <strong>MSSQL</strong>. The database type must be the same as the database type selected for the MDM Hub Master Database and the Operational Reference Stores.</td>
</tr>
<tr>
<td>ActiveVOS User Name</td>
<td>User name of the ActiveVOS Server administrative user.</td>
</tr>
<tr>
<td>ActiveVOS User Password</td>
<td>Password of the administrative user.</td>
</tr>
<tr>
<td>ActiveVOS Collation Name</td>
<td>Name of the ActiveVOS database collation. For example, <strong>Latin1_General_CI_AS</strong>.</td>
</tr>
<tr>
<td>ActiveVOS Database Host Name</td>
<td>Name of the machine that hosts the database.</td>
</tr>
<tr>
<td>ActiveVOS Database Path</td>
<td>Path to the database location.</td>
</tr>
<tr>
<td>DBA User Name</td>
<td>User name of the SA user.</td>
</tr>
<tr>
<td>DBA Password</td>
<td>Password of the SA user account.</td>
</tr>
</tbody>
</table>

4. After you create the schema, review the **sip_ant.log** file in the following directory:

   `<MDM Hub distribution directory>/database/bin`

   The **sip_ant.log** file logs any errors that might occur when you run the **sip_ant** script to create the ActiveVOS database schema.
CHAPTER 4

Application Server Tasks

This chapter includes the following topics:

- Application Server Tasks Overview, 44
- Set Up JBoss, 44
- Set Up Oracle WebLogic, 50
- Additional Oracle WebLogic Configuration, 54
- Set Up IBM WebSphere, 58
- Additional IBM WebSphere Configuration, 63

Application Server Tasks Overview

Configure your application server to work with Multidomain MDM. Follow the instructions for your application server.

When you perform a clean upgrade, perform all the steps for your application server as you would for a new installation of Multidomain MDM.

When you perform an in-place upgrade where your application server is still supported, verify that the application server is configured to work with this version of Multidomain MDM.

Set Up JBoss

You can install the MDM Hub in a JBoss cluster environment or on standalone JBoss instances. Install and configure JBoss according to the instructions in the JBoss documentation. Whether you install the MDM Hub in a JBoss cluster environment or on standalone JBoss instances, install the JBoss standalone configuration, and use the full profile of the configuration.

A JBoss cluster consists of one or more cluster nodes on one or more machines. Install and configure JBoss on all machines on which you want cluster nodes. In a cluster environment, ensure that the directory structure of the JBoss installations is the same on all the cluster nodes.

**Note:** Install the application server in the same time zone as the database server.
Configure Java Virtual Machines

To configure a Java Virtual Machine (JVM), set Java options by using the JAVA_OPTS environment variable.

You can set the Java options in the following file:

On UNIX. `<JBoss installation directory>/bin/standalone.conf`

On Windows. `<JBoss installation directory>\bin\standalone.conf.bat`

The following table describes the Java options settings:

<table>
<thead>
<tr>
<th>Java Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-server</td>
<td>Results in a slower startup but subsequent operations are faster.</td>
</tr>
<tr>
<td>-Ddb2.jcc.charsetDecoderEncoder</td>
<td>Required to use the MDM Hub Sample Operational Reference Store. Enables the JDBC driver to return the Unicode replacement character (U+FFFD) in place of a sequence of bytes that is not a UTF-8 string. Set to 3.</td>
</tr>
<tr>
<td>-Djava.net.preferIPv4Stack</td>
<td>Specifies whether Java uses Internet Protocol version 4 (IPv4). If the operating system uses Internet Protocol version 6 (IPv6), set to true.</td>
</tr>
<tr>
<td>-Djboss.as.management.blocking.timeout</td>
<td>Time in seconds to wait for JBoss to deploy. To ensure that JBoss does not fail to start, you can set the value to 5000. Adjust the time period based on your environment. Default is 300. If you do not configure the parameter, you might encounter a JBoss deployment timeout.</td>
</tr>
</tbody>
</table>
| -Djavax.net.ssl.trustStore=<Security certificate key file path>  
-Djavax.net.ssl.trustStorePassword=<keystore password>" | Imports the security certificate. Required if you want to configure the HTTPS protocol for the MDM Hub communications and for the ActiveVOS communications with the MDM Hub. Before you configure the property, use the Java keytool command to generate a keystore and an alias. If you use a certificate chain, the alias of the end-user certificate must be the same as the application server host name. |
| -Djgroups.bind_addr                               | Interface on which JGroup must receive and send messages. Required in multinode or cluster environments. Ensure that each node binds to its own network interface. |
| -DFrameworksLogConfigurationPath                  | Path to the log4j.xml file.                                                                 |
| -Dmdm.node.groupid                                | Specifies a group ID for Java Virtual Machines in the MDM Hub implementation. Required only if you want logical groupings of Hub Servers and Process Servers. |
### Java Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-Dorg.apache.catalina.connector.URI_ENCODING</code></td>
<td>Required if you want to use Informatica Data Director and use REST APIs to search for records. Set to $\text{UTF-8}$ to ensure that you can find and save records that contain UTF-8 characters.</td>
</tr>
<tr>
<td><code>-Dtask.pageSize=&lt;maximum number of tasks&gt;</code></td>
<td>Specifies the maximum number of ActiveVOS tasks that are retrieved for each request. Default is 5000. Increase the number if your environment has a large number of tasks.</td>
</tr>
<tr>
<td><code>-Dstricttransportsecurity.flag</code></td>
<td>Specifies whether web browsers must convert all attempts to access Informatica Data Director using the HTTP requests to the HTTPS requests instead. Set to $\text{true}$.</td>
</tr>
<tr>
<td><code>-Xms</code></td>
<td>Initial heap size. Set to 2048m.</td>
</tr>
<tr>
<td><code>-Xmx</code></td>
<td>Maximum JVM heap size. Set to 4 GB or higher. For example, to set the <code>-Xmx</code> to 4096m, use the following JAVA_OPTIONS environment variable setting: set &quot;$\text{JAVA_OPTIONS}=\text{-server } \text{-Xmx4096m}$&quot;</td>
</tr>
<tr>
<td><code>XX:+UseCodeCacheFlushing</code></td>
<td>Specifies whether the JVM disposes of compiled code when the code cache is full.</td>
</tr>
<tr>
<td><code>-XX:ReservedCodeCacheSize</code></td>
<td>JIT code cache size. To enhance the performance of the MDM Hub environment, set to 512m.</td>
</tr>
</tbody>
</table>

### Logical Grouping of Java Virtual Machine Example

By grouping Java Virtual Machines (JVMs), you get a logical group of Hub Servers and Process Servers. When you deploy the Hub Server and Process Server applications in a logical JVM group, all communication between the applications stays within the group. To group JVMs, you assign a group ID to each JVM in the MDM Hub environment.

**Note:** Process Server grouping is applicable to the cleanse and match process only. A Process Server that is enabled as a Zookeeper server and is enabled for smart search is available to all the groups for indexing and search processing.

The following table shows an example of logical JVM groups:

<table>
<thead>
<tr>
<th>JVM Group</th>
<th>JVM</th>
<th>Hub Server</th>
<th>Process Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>JVM1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group1</td>
<td>JVM4</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Configure Server Properties for the Full Profile

Configure the server properties for the full profile of the standalone mode in the `standalone-full.xml` file.

The `standalone-full.xml` file is in the following directory:

`<JBoss installation directory>/standalone/configuration`

The following table describes the server properties configuration for the full profile:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction timeout</td>
<td>Ensures that the MDM Hub transactions complete. In the <code>subsystem</code> with the name `urn:jboss:domain:transactions:&lt;n.n.&gt;, set default-timeout=3600 for the coordinator-environment element.</td>
</tr>
</tbody>
</table>
| HTTPS protocol      | Required if you want to configure the HTTPS protocol for the MDM Hub communications and for ActiveVOS communications with the MDM Hub. **Note:** Before you configure the HTTPS protocol, use the Java keytool command to generate a keystore and an alias. Note the key alias and keystore password that you create.  
To configure the HTTPS protocol, in the `subsystem` with the name `urn:jboss:domain:web:<n.n.>, add the following `connector` configuration:  
```xml  
<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">  
  <ssl name="ssl" key-alias="<Key alias>" password="<keystore password>" certificate-key-file="<Security certificate key file path>" protocol="TLSv1" verify-client="false"/>  
</connector>  
``` |
Create the ActiveVOS Console Administrative User

If you want to use ActiveVOS, create the ActiveVOS Console administrative user with the `abAdmin` role in the application server container. If you want to use ActiveVOS, create the ActiveVOS Console administrative user with the `abAdmin` role. If you do not create an administrative user, the Hub Server deployment fails. Use the ActiveVOS Console administrative user name and password when the Hub Server installer prompts you to enter the administrative user credentials for the ActiveVOS Console.

1. Change to the following directory:
   
   `<JBoss installation directory>/bin`

2. To run the add-user utility, use the following script:

   On UNIX, `add-user.sh`
   
   On Windows, `add-user.bat`

3. Answer the prompts that appear.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HornetQ Security</td>
<td>If HornetQ security is enabled for the JBoss server, disable it. In the <code>hornetq-server</code> element, set the <code>security-enabled</code> configuration to false as shown in the following example:</td>
</tr>
<tr>
<td>Remoting-connector security</td>
<td>Configures remoting-connector security. To log in to the Hub Console from a remote machine, disable the remoting-connector security. In the <code>subsystem</code> with the name <code>urn:jboss:domain:remoting:&lt;n.n&gt;</code>, remove the <code>security-realm</code> attribute from the following <code>connector</code> configuration:</td>
</tr>
<tr>
<td>Asynchronous handling of loggers</td>
<td>If the JBoss environment runs on Java 1.7, and you want to use Informatica Data Director, configure asynchronous handling of loggers. In the <code>subsystem</code> with the name <code>urn:jboss:domain:logging:&lt;n.n&gt;</code>, add the following async-handler configuration:</td>
</tr>
<tr>
<td>Port configuration for JBoss instances</td>
<td>If you want to install multiple MDM Hub instances on the same machine, you deploy each MDM Hub instance on a separate JBoss instance. To avoid port conflicts, for each JBoss instance, set the <code>port-offset</code> attribute of the <code>socket-binding-group</code> element to a different value.</td>
</tr>
<tr>
<td>Access to the JBoss root welcome page</td>
<td>Disable access to the JBoss root welcome page. For instructions, see the JBoss documentation.</td>
</tr>
</tbody>
</table>
The following table describes the values to specify for each prompt:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value to Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of user do you wish to add? a) Management User or b) Application User</td>
<td>To select Application User, enter b.</td>
</tr>
<tr>
<td>Realm (ApplicationRealm)</td>
<td>Realm name. Enter the realm name that you specified in the login-module that you added to the standalone-full.xml file.</td>
</tr>
<tr>
<td>Username</td>
<td>ActiveVOS Console administrator name.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that complies with the JBoss password standard.</td>
</tr>
<tr>
<td>What roles do you want this user to belong to?</td>
<td>abAdmin.</td>
</tr>
<tr>
<td>About to add user &lt;user name&gt; for realm &lt;realm name&gt;. Is this correct?</td>
<td>To add the user, enter yes.</td>
</tr>
<tr>
<td>Is this new user going to be used for one AS process to connect to another AS process?</td>
<td>yes.</td>
</tr>
</tbody>
</table>

4. Log in to the WebSphere console, and create the ActiveVOS Console administrative user.

   **Note:** The ActiveVOS console user is mapped to the abAdmin role when you run the postInstallSetup or the patchInstallSetup script during the post-installation or post-upgrade process.

5. Log in to the WebLogic console.
6. Create the abAdmin role.
7. Create the ActiveVOS Console administrative user.
8. Assign the administrative user to the abAdmin role

**Start JBoss**

Before you install the Hub Server and the Process Server, start the JBoss application server. Based on your environment, you either start standalone JBoss instances or JBoss cluster nodes.

**Starting Standalone JBoss Instances**

If you use standalone JBoss instances, start each instance on which you want to install the MDM Hub components.

1. Navigate to the following directory:
   
   `<JBoss installation directory>/bin`

2. To start a JBoss instance, run the following command:
   
   On **UNIX**, `standalone.sh -c standalone-full.xml -b 0.0.0.0 -Djboss.as.management.blocking.timeout=5000`
   
   On **Windows**, `standalone.bat -c standalone-full.xml -b 0.0.0.0 -Djboss.as.management.blocking.timeout=5000`
JBoss starts on the available network interfaces and listens for the current host that is defined in the hosts file in the /etc/hosts directory. Adjust the timeout interval based on your environment.

3. If you have multiple JBoss instances on the same machine, to start the second and any subsequent JBoss instances, add the following argument to the startup command:

-Djboss.service.binding.set=ports-01

Starting JBoss Cluster Nodes

If you use a JBoss cluster environment, start the cluster nodes on which you want to install the MDM Hub components.

1. Navigate to the following directory:

<JBoss installation directory>/bin

2. To start a JBoss cluster node, run the following command on machines that have cluster nodes:

On UNIX: standalone.sh -c standalone-full.xml -b 0.0.0.0 -Djboss.node.name=<Name of the cluster node> -Djboss.server.base.dir=../<node path> -Djboss.as.management.blocking.timeout=5000 -u <multicast address> -Djgroups.bind_addr=<bind address> -Djboss.socket.bindung.port-offset=<port offset value> -Djboss.partition.name=<Partition name>

On Windows: standalone.bat -c standalone-full.xml -b 0.0.0.0 -Djboss.node.name=<Name of the cluster node> -Djboss.server.base.dir=../<node path> -Djboss.as.management.blocking.timeout=5000 -u <multicast address> -Djgroups.bind_addr=<bind address> -Djboss.socket.bindung.port-offset=<port offset value> -Djboss.partition.name=<Partition name>

Set the port offset value if multiple cluster nodes run on the same machine. Use the default partition name or ensure that the partition name is the same for all nodes that belong to a cluster. Adjust the timeout interval based on your environment.

Set Up Oracle WebLogic

You can install the MDM Hub in an Oracle WebLogic cluster environment or on standalone WebLogic instances. Install and configure WebLogic according to the instructions in the WebLogic documentation.

Important: There are some known limitations with how Multidomain MDM interacts with some Oracle WebLogic versions, including version 12.2.1.3. Before you begin, see the "Installation and Upgrade" chapter of the Multidomain MDM Release Notes.

Before you install the Hub Server and the Process Server on the WebLogic application server, create WebLogic domains. Use the WebLogic Administration console to create domains for the Hub Server and the Process Server applications. For more information, see the WebLogic documentation.

Note: Install the application server in the same time zone as the database server.

Configure the Java Virtual Machines

To configure a Java Virtual Machine (JVM), set the Java options by using the the JAVA_OPTIONS environment variable.

You can set the Java options in the following file:
On UNIX. `<WebLogic domain>/bin/setDomainEnv.sh`

On Windows. `<WebLogic domain>\bin\setDomainEnv.cmd`

The following table describes the Java options:

<table>
<thead>
<tr>
<th>Java Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-server</td>
<td>Results in a slower startup but subsequent operations are faster.</td>
</tr>
<tr>
<td>-Djgroups.bind_addr</td>
<td>Interface on which JGroup must receive and send messages. Required in a multinode or clustered environment. Ensure that each node binds to its own network interface.</td>
</tr>
<tr>
<td>-Djava.net.preferIPv4Stack</td>
<td>Specifies whether Java uses Internet Protocol version 4 (IPv4). If the operating system uses Internet Protocol version 6 (IPv6), set to <code>true</code>.</td>
</tr>
<tr>
<td>-Doracle.jdbc.J2EE13Compliant</td>
<td>Sets the <code>oracle.jdbc.J2EE13Compliant</code> system variable. Set to <code>true</code>. If you do not set the parameter to <code>true</code>, you might encounter Java Database Connectivity (JDBC) issues.</td>
</tr>
<tr>
<td>-Djavax.wsdl.factory.WSDLFactory</td>
<td>Required for the WebLogic 12.2.1 or later environments to invoke a service WSDL that might have a default namespace prefix. Set to <code>com.ibm.wsdl.factory.WSDLFactoryImpl</code>.</td>
</tr>
<tr>
<td>-DANTLR_USE_DIRECT_CLASS_LOADING</td>
<td>Required for launching WebLogic 12.2.1 or later environments on which the MDM Hub is deployed. Set to <code>true</code>.</td>
</tr>
<tr>
<td>-Dmdm.node.groupid</td>
<td>Specifies a group ID for Java Virtual Machines in the MDM Hub implementation. Required only if you want logical groupings of Hub Servers and Process Servers.</td>
</tr>
<tr>
<td>-De360.mdm.host</td>
<td>Application server host. Set the Java option in one of the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>- If you want to deploy the MDM Hub applications only on Managed Servers, add the Java option to the script of each Managed Server. Set to the IP address or symbolic name of the Managed Server.</td>
</tr>
<tr>
<td></td>
<td>- If you want to deploy the MDM Hub applications on a WebLogic port other than 7001, add the Java option to the application server startup script. Set to the IP address or symbolic name of the WebLogic host. If you do not configure this parameter, Informatica Data Director screens based on the Entity 360 Framework might not work as expected.</td>
</tr>
<tr>
<td>-De360.mdm.port</td>
<td>Application server port. Set the Java option in one of the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>- If you want to deploy the MDM Hub applications only on Managed Servers, add the Java option to the script of each Managed Server. Set to the port number of the Managed Server.</td>
</tr>
<tr>
<td></td>
<td>- If you want to deploy the MDM Hub applications on a WebLogic port other than 7001, add the Java option to the application server startup script and set to the port number. If you do not configure this parameter, Informatica Data Director screens based on the Entity 360 Framework might not work as expected.</td>
</tr>
<tr>
<td>-Dfile.encoding</td>
<td>Required if you want to use Informatica Data Director and use REST APIs to search for records. Set both the Java options to <code>UTF-8</code> to ensure that you can find and save records that contain UTF-8 characters.</td>
</tr>
<tr>
<td>-Dweblogic.http.URIDecodeEncoding</td>
<td></td>
</tr>
</tbody>
</table>
**Java Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-DFrameworksLogConfigurationPath</code></td>
<td>Sets the log4j.xml file configuration path.</td>
</tr>
<tr>
<td><code>-DUseSunHttpHandler</code></td>
<td>Specifies whether WebLogic uses the Sun HTTP Handler for the HTTP connection between the MDM Hub and the Informatica platform. Set to <code>true</code>.</td>
</tr>
<tr>
<td><code>-Dtask.pageSize=&lt;maximum number of tasks&gt;</code></td>
<td>Specifies the maximum number of ActiveVOS tasks that are retrieved for each request. Default is <code>5000</code>. Increase the number if your environment has a large number of tasks.</td>
</tr>
<tr>
<td><code>-Dstricttransportsecurity.flag</code></td>
<td>Specifies whether web browsers must convert all attempts to access Informatica Data Director using the HTTP requests to the HTTPS requests instead. Set to <code>true</code>.</td>
</tr>
<tr>
<td><code>WLS_MEM_ARGS_64BIT</code></td>
<td>Memory variable. Set the variable to an appropriate value.</td>
</tr>
<tr>
<td><code>-Xms</code></td>
<td>Initial heap size. Set to <code>2048m</code>.</td>
</tr>
</tbody>
</table>
| `-Xmx` | Maximum JVM heap size. Set to `4 GB` or higher. For example, to set the `-Xmx` to `4096m`, use the following JAVA_OPTIONS environment variable setting:  
  ```
  set "JAVA_OPTIONS=-server ...
  -Xmx4096m"
  ``` |
| `-XX:+UseCodeCacheFlushing` | Specifies whether the JVM disposes of compiled code when the code cache is full. |
| `-XX:ReservedCodeCacheSize` | JIT code cache size. To enhance the performance of the MDM Hub environment, set to `512m`. |

**Logical Grouping of Java Virtual Machine Example**

By grouping Java Virtual Machines (JVMs), you get a logical group of Hub Servers and Process Servers. When you deploy the Hub Server and Process Server applications in a logical JVM group, all communication between the applications stays within the group. To group JVMs, you assign a group ID to each JVM in the MDM Hub environment.

**Note:** Process Server grouping is applicable to the cleanse and match process only. A Process Server that is enabled as a Zookeeper server and is enabled for smart search is available to all the groups for indexing and search processing.

The following table shows an example of logical JVM groups:

<table>
<thead>
<tr>
<th>JVM Group</th>
<th>JVM</th>
<th>Hub Server</th>
<th>Process Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>JVM1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group1</td>
<td>JVM4</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Group2</td>
<td>JVM2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group3</td>
<td>JVM3</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>
For JVM1, add the following Java option in the startup script:
-Dmmdm.node.groupid=Group1

For JVM2, add the following Java option in the startup script:
-Dmmdm.node.groupid=Group2

For JVM3, add the following Java option in the startup script:
-Dmmdm.node.groupid=Group3

For JVM4, add the following Java option in the startup script:
-Dmmdm.node.groupid=Group1

After you configure the JVMs, and deploy the Hub Servers and Process Servers, the groups have the following characteristics:

- Group1 has two Process Servers, Group2 has one Process Server, and Group3 has one Process Server.
- All cleanse and batch calls stay in their own group with the exception of smart search. For example, any real-time call on the Hub Server in Group1 affects only the Group1 Process Servers (JVM1 and JVM4).

**Disable WebLogic Server Authentication**

The MDM Hub uses HTTP basic authentication for which you must disable WebLogic Server authentication. To disable WebLogic Server authentication, edit the config.xml file.

1. Navigate to the following WebLogic directory:
   
   `<WebLogic installation directory>/user_projects/domains/<user domain>/config`

2. Open the config.xml file in a text editor.

3. Add the following element within the `<security-configuration>` element:

   ```
   <enforce-valid-basic-auth-credentials>
   false
   </enforce-valid-basic-auth-credentials>
   ```

**Create the ActiveVOS Console Administrative User**

If you want to use ActiveVOS, create the ActiveVOS Console administrative user with the abAdmin role in the application server container. If you want to use ActiveVOS, create the ActiveVOS Console administrative user with the abAdmin role. If you do not create an administrative user, the Hub Server deployment fails. Use the ActiveVOS Console administrative user name and password when the Hub Server installer prompts you to enter the administrative user credentials for the ActiveVOS Console.

1. Change to the following directory:

   `<JBoss installation directory>/bin`

2. To run the add-user utility, use the following script:

   - On UNIX, `add-user.sh`
   - On Windows, `add-user.bat`

3. Answer the prompts that appear.
The following table describes the values to specify for each prompt:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value to Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of user do you wish to add? a) Management User or b) Application User</td>
<td>To select Application User, enter b.</td>
</tr>
<tr>
<td>Realm (ApplicationRealm)</td>
<td>Realm name. Enter the realm name that you specified in the login-module that you added to the standalone-full.xml file.</td>
</tr>
<tr>
<td>Username</td>
<td>ActiveVOS Console administrator name.</td>
</tr>
<tr>
<td>Password</td>
<td>Password that complies with the JBoss password standard.</td>
</tr>
<tr>
<td>What roles do you want this user to belong to?</td>
<td>abAdmin.</td>
</tr>
<tr>
<td>About to add user &lt;user name&gt; for realm &lt;realm name&gt;. Is this correct?</td>
<td>To add the user, enter yes.</td>
</tr>
<tr>
<td>Is this new user going to be used for one AS process to connect to another AS process?</td>
<td>yes.</td>
</tr>
</tbody>
</table>

4. Log in to the WebSphere console, and create the ActiveVOS Console administrative user.  
   **Note:** The ActiveVOS console user is mapped to the abAdmin role when you run the postInstallSetup or the patchInstallSetup script during the post-installation or post-upgrade process.

5. Log in to the WebLogic console.
6. Create the abAdmin role.
7. Create the ActiveVOS Console administrative user.
8. Assign the administrative user to the abAdmin role

### Additional Oracle WebLogic Configuration

Perform additional WebLogic configuration based on the requirements of the MDM Hub environment.

The following table describes the configurations that you can perform:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configuring WebLogic for standalone Process Server instances | Required to configure WebLogic for standalone Process Server instances in the following scenarios:  
  - You want to install a Process Server instance on a WebLogic instance on which you do not have the Hub Server installed.  
  - You want to install multiple, standalone Process Server instances. |
<p>| Configuring WebLogic for multiple MDM Hub Master Databases  | Required if you want to configure multiple MDM Hub Master Database instances.                                                             |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the HTTPS protocol</td>
<td>Required if you want to configure the HTTPS protocol for the MDM Hub</td>
</tr>
<tr>
<td>communications.</td>
<td></td>
</tr>
<tr>
<td>Configuring the JTA timeout for</td>
<td>Required if you want to install Informatica platform.</td>
</tr>
<tr>
<td>Informatica platform</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring WebLogic for Standalone Process Server Instances

If you want to install multiple, standalone Process Server instances, configure WebLogic to use the appropriate data source. Also, if you want to install a Process Server instance on a WebLogic instance on which you do not have the Hub Server installed, configure the data source.

Perform the following tasks to configure WebLogic to use the appropriate data source:

1. Install the JDBC driver.
2. Create an MDM Hub Master Database data source.
3. Create an Operational Reference Store data source.

#### Step 1. Install the JDBC Driver

Before you create data sources for the MDM Hub Master Database and the Operational Reference Store (ORS), install the JDBC driver.

Contact Oracle to get the supported version of the JDBC driver.

Contact Microsoft to get the supported version of the JDBC driver.

Contact IBM to get the supported version of the JDBC driver.

1. Copy the JDBC driver to the following directory:
   
   `<WebLogic installation directory>/wlsserver/server/lib`

2. Add the path to the JDBC driver to the `CLASSPATH` variable in the following file:
   
   **On UNIX.** `<WebLogic domain>/bin/setDomainEnv.sh`
   
   **On Windows.** `<WebLogic domain>/bin\setDomainEnv.cmd`

   **Note:** Place the path to the JDBC driver before the path to other Weblogic Server libraries.

#### Step 2. Create an MDM Hub Master Database Data Source

After you install the JDBC driver, on the Process Server machine, create a data source for the MDM Hub Master Database.

1. On the WebLogic Administration Console, click the **Lock & Edit** button to acquire a lock.
2. Click **Services > JDBC > Data Sources**, and then click **New**.
   
   The **JDBC Data Sources Properties** page appears.
3. Specify the following data source properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the JDBC data source. Set the name to MDM Master Data Source.</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>JNDI path to where the JDBC data source will be bound. Specify jdbc/siperian-cmx_system-ds.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Database type that you want to connect to. Select Oracle. Select MS SQL Server.</td>
</tr>
<tr>
<td>Database Driver</td>
<td>JDBC driver that you want to use to connect to the database. Select Oracle driver (Thin XA). Select MS SQL Server Driver (Type 4 XA) Versions: 2005 or later.</td>
</tr>
</tbody>
</table>

4. Click Next, and again click Next.

   The Connection Properties page appears.

5. Enter values for the following connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>Name of the database you want to connect to.</td>
</tr>
<tr>
<td>Host Name</td>
<td>DNS name or IP address of the server that hosts the database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on which the database server listens for connection requests.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>Database user name that you want to use for each connection in the data source.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the database user account.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Password of the database user account.</td>
</tr>
</tbody>
</table>

6. Click Next.

   The Test Database Connection page appears.

7. Click Test Configuration to test the driver connections.

   If the test is unsuccessful, you must update the values in the Connection Properties page and then retry the connection until successful.

8. Click Next, and then select the server on which you want to deploy the data source.

9. Click Finish, and then click Activate Changes.

Step 3. Create an Operational Reference Store Data Source

On the Process Server machine, create a data source for each Operational Reference Store.

1. On the WebLogic Administration Console, click the Lock & Edit button to acquire a lock.

2. Click Services > JDBC > Data Sources, and then click New.

   The JDBC Data Sources Properties page appears.
3. Specify the following data source properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the JDBC data source. Set the name to MDM ORS Data Source.</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>JNDI path to where the JDBC data source will be bound. Specify jdbc/siperian-&lt;oracle host name&gt;-&lt;oracle sid&gt;-&lt;Operational reference Store name&gt;-ds. Specify jdbc/siperian-&lt;Microsoft SQL Server host name&gt;-&lt;Operational reference Store name&gt;-ds.</td>
</tr>
<tr>
<td>Database Type</td>
<td>Database type that you want to connect to. Select Oracle. Select MS SQL Server.</td>
</tr>
<tr>
<td>Database Driver</td>
<td>JDBC driver that you want to use to connect to the database. Select Oracle driver (Thin XA). Select MS SQL Server Driver (Type 4 XA) Versions: 2005 or later.</td>
</tr>
</tbody>
</table>

4. Click Next, and again click Next.

The Connection Properties page appears.

5. Enter values for the following connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Name</td>
<td>Name of the database you want to connect to.</td>
</tr>
<tr>
<td>Host Name</td>
<td>DNS name or IP address of the server that hosts the database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port on which the database server listens for connection requests.</td>
</tr>
<tr>
<td>Database User Name</td>
<td>Database user name that you want to use for each connection in the data source.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the database user account.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Password of the database user account.</td>
</tr>
</tbody>
</table>

6. Click Next.

The Test Database Connection page appears.

7. Click Test Configuration to test the driver connections.

If the test is unsuccessful, you must update the values in the Connection Properties page and then retry the connection until successful.

8. Click Next, and then select the server on which you want to deploy the data source.

9. Click Finish, and then click Activate Changes.

Configuring WebLogic for Multiple MDM Hub Master Databases

If you want to configure multiple MDM Hub Master Database instances, configure as many WebLogic domains as the number of MDM Hub Master Database instances. Each MDM Hub Master Database instance must have its own MDM Hub instance. Therefore, create as many WebLogic domains to deploy each MDM Hub instance on a separate WebLogic domain.
Configuring the HTTPS Protocol

You can configure the HTTPS protocol for the MDM Hub communications. Use the WebLogic Server Administration Console to configure the HTTPS protocol. Alternatively, you can use the default JDK secure certificates to enable HTTPS.

1. On the Home Page of the WebLogic Server Administration Console, under the Environment section, click Servers.
   The Summary of Servers page appears.
2. In the Servers list, click the AdminServer(admin) link.
   The Settings for AdminServer page appears.
3. Enable the SSL Listen Port Enabled option, and enter the port number in the SSL Listen Port field.
4. Click the SSL tab.
5. From the Hostname Verification list, select None, and click Save.

Configuring the JTA Timeout for Informatica Platform

If you want to install Informatica platform, configure the Java Transaction API (JTA) timeout. Use the WebLogic Server Administration Console to configure the JTA timeout.

1. On the Home Page of the WebLogic Server Administration Console, under the Services Configurations section, click the JTA Configuration link.
2. In the Timeout Seconds field, set the JTA timeout to 1000.

Set Up IBM WebSphere

You can install the MDM Hub in IBM WebSphere cluster environments or standalone WebSphere instances. Install and configure WebSphere according to the instructions in the WebSphere documentation.

Ensure that there are no white spaces in the WebSphere installation directory path.

Note: Install the application server in the same time zone as the database server.

The following table lists the properties and their values to configure before installation, followed by a brief description of where to set the property:

<table>
<thead>
<tr>
<th>Custom Property</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.ibm.ws.scripting.echoparams        | false | Set this property in the wsadmin.properties file, which is located the following directory: <WebSphere installation directory> \WebSphere\AppServer\profiles\<profile name> \properties  
Set this value to false to prevent the ActiveVOS database password from appearing in script text in the patchinstallSetup.log file. Default is true. |
Configure Java Virtual Machines

To configure a Java Virtual Machine (JVM), set Java options by using the JAVA_OPTIONS environment variable. After you edit or add any Java options, restart the JVM.

If you use a WebSphere clustered environment, set the Java options for the following cluster components:

- Server. Set all the required Java options on each server in the cluster.
- Deployment Manager. Set all the required Java options.
- Node agent. Set only heap size by using the -Xmx and -Xms Java options.

The following table describes the Java options settings:

<table>
<thead>
<tr>
<th>Java Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-server</td>
<td>Results in a slower startup but subsequent operations are faster.</td>
</tr>
<tr>
<td>-Djava.net.preferIPv4Stack</td>
<td>Specifies whether Java uses Internet Protocol version 4 (IPv4). If the</td>
</tr>
<tr>
<td></td>
<td>operating system uses Internet Protocol version 6 (IPv6), set to true.</td>
</tr>
<tr>
<td>-Ddb2.jcc.charsetDecoderEncoder</td>
<td>Required to use the MDM Hub Sample Operational Reference Store. Enables the</td>
</tr>
<tr>
<td></td>
<td>JDBC driver to return the Unicode replacement character (U+FFFD) in place</td>
</tr>
<tr>
<td></td>
<td>of a sequence of bytes that is not a UTF-8 string. Set to 3.</td>
</tr>
<tr>
<td>-Dcom.ibm.crypto.provider.DoRSATypeChecking</td>
<td>Specifies whether Java allows the RSA type encryption of data with private</td>
</tr>
<tr>
<td></td>
<td>key and decryption with public key. Required for the MDM Hub installer to</td>
</tr>
<tr>
<td></td>
<td>read the license certificates and for password hashing to work in the MDM</td>
</tr>
<tr>
<td></td>
<td>Hub. Set to false.</td>
</tr>
<tr>
<td></td>
<td>If you do not set -Dcom.ibm.crypto.provider.DoRSATypeChecking to false, the</td>
</tr>
<tr>
<td></td>
<td>Hub Server might not start and you can encounter license errors.</td>
</tr>
<tr>
<td>-Djgroups.bind_addr</td>
<td>Interface on which JGroup must receive and send messages. Required in a</td>
</tr>
<tr>
<td></td>
<td>multinode or clustered environment. Ensure that each node binds to its own</td>
</tr>
<tr>
<td></td>
<td>network interface.</td>
</tr>
<tr>
<td>-DFrameworksLogConfigurationPath</td>
<td>Path to the log4j.xml file.</td>
</tr>
<tr>
<td>-Doracle.jdbc.J2EE13Compliant</td>
<td>Specifies whether the system variable for the Oracle driver is fully</td>
</tr>
<tr>
<td></td>
<td>compliant with J2EE. Set to true.</td>
</tr>
<tr>
<td></td>
<td>If you do not set the parameter to true, you might encounter Java Database</td>
</tr>
<tr>
<td></td>
<td>Connectivity (JDBC) issues</td>
</tr>
<tr>
<td>-Dmdm.node.groupid</td>
<td>Specifies a group ID for Java Virtual Machines in the MDM Hub</td>
</tr>
<tr>
<td></td>
<td>implementation. Required only if you want logical groupings of Hub</td>
</tr>
<tr>
<td></td>
<td>Servers and Process Servers.</td>
</tr>
<tr>
<td>-Djavax.management.builder.initial</td>
<td>Class of the initial MBeanServerBuilder to be instantiated. Apache Solr</td>
</tr>
<tr>
<td></td>
<td>MBeans is required to support smart search in Informatica Data Director.</td>
</tr>
<tr>
<td></td>
<td>To register Apache Solr MBeans to support smart search in Informatica Data</td>
</tr>
<tr>
<td></td>
<td>Director, set to javax.management.MBeanServerBuilder.</td>
</tr>
</tbody>
</table>
### Java Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Dfile.encoding</td>
<td>Required if you want to use Informatica Data Director and use REST APIs to search for records. Set both the Java options to UTF-8 to ensure that you can find and save records that contain UTF-8 characters.</td>
</tr>
<tr>
<td>-Dclient.encoding.override</td>
<td></td>
</tr>
<tr>
<td>-Dstricttransportsecurity.flag</td>
<td>Specifies whether web browsers must convert all attempts to access Informatica Data Director using the HTTP requests to the HTTPS requests instead. Set to true.</td>
</tr>
<tr>
<td>-XX:codecachetotal</td>
<td>JIT code cache size. To enhance the performance of the MDM Hub environment, set to 512m.</td>
</tr>
<tr>
<td>-Xmx</td>
<td>Maximum JVM heap size. Set to 4 GB or higher. For example, to set the -Xmx to 4096m, use the following JAVA_OPTIONS environment variable setting: set &quot;JAVA_OPTIONS=-server ... -Xmx4096m&quot;</td>
</tr>
<tr>
<td>-Xms</td>
<td>Initial heap size. Set to 2048m.</td>
</tr>
<tr>
<td>-XmsO</td>
<td>Required for the Process Server JVMs. Initial stack size for operating system threads. Prevents the application server from shutting down unexpectedly due to low system thread stack size. Set to 4096k.</td>
</tr>
<tr>
<td>-Xss</td>
<td>Initial stack size. Set to 2000k.</td>
</tr>
<tr>
<td>XX:+UseCodeCacheFlushing</td>
<td>Specifies whether the JVM disposes of compiled code when the code cache is full.</td>
</tr>
<tr>
<td>-Dtask.pageSize=&lt;maximum number of tasks&gt;</td>
<td>Specifies the maximum number of ActiveVOS tasks that are retrieved for each request. Default is 5000. Increase the number if your environment has a large number of tasks.</td>
</tr>
</tbody>
</table>

### Logical Grouping of Java Virtual Machine Example

By grouping Java Virtual Machines (JVMs), you get a logical group of Hub Servers and Process Servers. When you deploy the Hub Server and Process Server applications in a logical JVM group, all communication between the applications stays within the group. To group JVMs, you assign a group ID to each JVM in the MDM Hub environment.

**Note:** Process Server grouping is applicable to the cleanse and match process only. A Process Server that is enabled as a Zookeeper server and is enabled for smart search is available to all the groups for indexing and search processing.

The following table shows an example of logical JVM groups:

<table>
<thead>
<tr>
<th>JVM Group</th>
<th>JVM</th>
<th>Hub Server</th>
<th>Process Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>JVM1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group1</td>
<td>JVM4</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Create a Secure Profile in a WebSphere Environment**

In WebSphere, configure a secure profile to use with Multidomain MDM and Informatica ActiveVOS.

1. From a command line, create a secure profile as shown in the following sample code:
   
   **On Windows**
   ```
   <app_server_root>\bin\manageprofiles.bat -create -profileName AppSrv01
   -profilePath <app_server_root>\profiles\AppSrv01
   -templatePath <app_server_root>\profileTemplates\default
   -adminUserName administrator -adminPassword password1 -enableAdminSecurity true
   ```
   
   **On UNIX**
   ```
   <app_server_root>/bin/manageprofiles.sh -create -profileName AppSrv01
   -profilePath <app_server_root>/profiles/AppSrv01
   -templatePath <app_server_root>/profileTemplates/default
   -adminUserName administrator -adminPassword password1 -enableAdminSecurity true
   ```
   
   2. In the WebSphere console, change the security Transport type to SSL-Supported.
      
      a. Expand **Security** and click **Global Security**.

---

<table>
<thead>
<tr>
<th>JVM Group</th>
<th>JVM</th>
<th>Hub Server</th>
<th>Process Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group2</td>
<td>JVM2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group3</td>
<td>JVM3</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Encrypt Passwords in the MDM Hub Environment**

To encrypt sensitive data such as passwords that appear in log files in the MDM Hub environment, configure scripting administration in WebSphere.

1. Open the `wsadmin.properties` file in the following directory:
   ```
   <WebSphere installation directory>/profiles/<Application server profile name>/properties
   ```
2. Set the `com.ibm.ws.scripting.echoparams` Java property to `false`. 

**For JVM1, add the following Java option in the startup script:**

```
-Dmdm.node.groupid=Group1
``` 

**For JVM2, add the following Java option in the startup script:**

```
-Dmdm.node.groupid=Group2
``` 

**For JVM3, add the following Java option in the startup script:**

```
-Dmdm.node.groupid=Group3
``` 

**For JVM4, add the following Java option in the startup script:**

```
-Dmdm.node.groupid=Group1
``` 

After you configure the JVMs, and deploy the Hub Servers and Process Servers, the groups have the following characteristics:

- Group1 has two Process Servers, Group2 has one Process Server, and Group3 has one Process Server.
- All cleanse and batch calls stay in their own group with the exception of smart search. For example, any real-time call on the Hub Server in Group1 affects only the Group1 Process Servers (JVM1 and JVM4).
b. Under Authentication, expand **RMI/IIOP security** and click **CSIv2 inbound communications**

c. Under CSIv2 Transport Layer, from the Transport list, select **SSL-Supported**.

d. Click **Apply**, and then click **Save**.

3. In the WebSphere console, ensure that application security is set.
   a. Expand **Security** and click **Global Security**.
   b. Under Application Security, select **Enable application security**.
   c. Click **Apply**, and then click **Save**.

4. Set up federated repositories.
   a. Expand **Security** and click **Global Security**.
   b. Under User account repository, from the Available realm definitions list, select **Federated repositories**.
   c. Click **Configure**.
   d. Under Repositories in the realm, click **Use built-in repository**.
   e. Specify a password for the administrative user.
   f. Click **Apply**, and then click **Save**.

5. Restart the WebSphere profile.

**Create the ActiveVOS Console Administrative User**

If you want to use ActiveVOS, create the ActiveVOS Console administrative user with the **abAdmin** role in the application server container. If you do not create an administrative user, the Hub Server deployment fails. Use the ActiveVOS Console administrative user name and password when the Hub Server installer prompts you to enter the administrative user credentials for the ActiveVOS Console.

1. Change to the following directory:
   `<jboss installation directory>/bin`

2. To run the add-user utility, use the following script:
   - On UNIX, `add-user.sh`
   - On Windows, `add-user.bat`

3. Answer the prompts that appear.
   The following table describes the values to specify for each prompt:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value to Specify</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of user do you wish to add? a) Management User or b) Application User</td>
<td>To select Application User, enter <strong>b</strong>.</td>
</tr>
<tr>
<td>Realm (ApplicationRealm)</td>
<td>Realm name. Enter the realm name that you specified in the login-module that you added to the standalone-full.xml file.</td>
</tr>
<tr>
<td>Username</td>
<td>ActiveVOS Console administrator name.</td>
</tr>
</tbody>
</table>
What roles do you want this user to belong to?

Password

Value to Specify

Password that complies with the JBoss password standard.

abAdmin.

To add the user, enter yes.

yes.

Is this new user going to be used for one AS process to connect to another AS process?

4. Log in to the WebSphere console, and create the ActiveVOS Console administrative user.

Note: The ActiveVOS console user is mapped to the abAdmin role when you run the postInstallSetup or the patchInstallSetup script during the post-installation or post-upgrade process.

5. Log in to the WebLogic console.

6. Create the abAdmin role.

7. Create the ActiveVOS Console administrative user.

8. Assign the administrative user to the abAdmin role

Configure SOAP Request Timeout for MDM Hub Deployments

To ensure that deployment of the MDM Hub components do not time out, set the SOAP request timeout property. After a successful installation, you can reset the property to its default value.

1. Open the soap.client.props file in the following directory:

   `<WebSphere installation directory>/profiles/<Application server profile name>/properties`

2. Set the com.ibm.SOAP.requestTimeout property to 1800 or higher.

Additional IBM WebSphere Configuration

Perform additional WebSphere configuration based on the requirements of the MDM Hub environment.

The following table describes the configurations that you can perform:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configuring WebSphere for standalone Process Server instances | Required to configure WebSphere for standalone Process Server instances in the following scenarios:  
  - You want to install a Process Server instance on a WebSphere instance on which you do not have the Hub Server installed.  
  - You want to install multiple, standalone Process Server instances.                      |
<p>| Configuring WebSphere for multiple MDM Hub Master Databases   | Required if you want to configure multiple MDM Hub Master Database instances.    |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the HTTPS protocol</td>
<td>Required if you want to configure the HTTPS protocol for the MDM Hub communications.</td>
</tr>
<tr>
<td>Configuring WebSphere for Informatica Data Director</td>
<td>Required if you want to use Data Director.</td>
</tr>
</tbody>
</table>

**Configuring WebSphere for Standalone Process Server Instances**

If you want to install multiple, standalone Process Server instances, configure WebSphere to use the appropriate data source. Also, if you want to install a Process Server instance on a WebSphere instance on which you do not have the Hub Server installed, configure the data source.

Perform the following tasks to configure WebSphere to use the appropriate data source:

1. Install the JDBC driver.
2. Create an MDM Hub Master Database data source.
3. Create an Operational Reference Store data source.

**Step 1. Install the JDBC Driver**

Before you create data sources for the MDM Hub Master Database and the Operational Reference Store (ORS), install the JDBC driver.

Contact Oracle to get the supported version of the JDBC driver.

Contact Microsoft to get the supported version of the JDBC driver.

Contact IBM to get the supported version of the JDBC driver.

- Copy the JDBC driver to the following directory:
  
  `<WebSphere installation directory>/lib`

**Step 2. Create an MDM Hub Master Database Data Source**

After you install the JDBC driver, on the Process Server machine, create a data source for the MDM Hub Master Database.

1. Start the WebSphere Application Server Administrative Console.
2. Specify the location of the driver libraries.
   a. Expand **Environment** in the console navigation tree.
   b. Click the **WebSphere Variables** link.
   c. Update the JDBC variable to point to the following JDBC driver directory:
      
      `<WebSphere installation directory>/lib`
3. Create the security account that the MDM Hub Master Database data source will use.
   a. Expand **Security** in the console navigation tree.
   b. Click the **Secure administration, applications, and infrastructure** link.
d. Click **New**, and specify the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Name of the MDM Hub Master Database.</td>
</tr>
<tr>
<td>User ID</td>
<td>User name to connect to the MDM Hub Master Database.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the MDM Hub Master Database.</td>
</tr>
</tbody>
</table>

e. Click **OK**.

4. Create the JDBC Provider.
   a. Expand **Resources > JDBC**, and then click **JDBC Providers**.
      The **JDBC Provider** page appears.
   b. Select the scope for applications to use the data source.
   c. Click **New**, and specify the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database type</td>
<td>Type of database. Select <strong>Oracle</strong>.</td>
</tr>
<tr>
<td>Provider type</td>
<td>Type of JDBC provider. Select <strong>Oracle JDBC Driver</strong>.</td>
</tr>
<tr>
<td>Implementation type</td>
<td>Data source implementation type. Select <strong>XA data source</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the JDBC provider. Change the name to <strong>Informatica MDM Oracle JDBC Provider (XA)</strong>.</td>
</tr>
</tbody>
</table>

d. Click **Next**, and then click **Finish**.

5. Create the MDM Hub Master Database data source.
   a. Click the JDBC provider that you created.
      The **Configuration** page appears.
   b. Under **Additional Properties**, click **Data sources**.
      The **Data Sources** page appears.
   c. Click **New**.
d. Specify the following data source properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Data source name. Specify MDM Master Data Source.</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>JNDI path to where the JDBC data source will be bound. Specify jdbc/siperian-cmx_system-ds. Note: The JNDI name must be in lower case.</td>
</tr>
<tr>
<td>Component-managed Authentication Alias</td>
<td>Authentication alias of the Master Database data source. Select &lt;host name&gt;/cmx_system.</td>
</tr>
</tbody>
</table>

e. Click Next, and then click Finish.

Step 3. Create an Operational Reference Store Data Source

After you install the JDBC driver, on the Process Server machine, create a data source for each Operational Reference Store.

1. Start the WebSphere Application Server Administrative Console.
2. Specify the location of the driver libraries.
   a. Expand Environment in the console navigation tree.
   b. Click the WebSphere Variables link.
   c. Update the JDBC variable to point to the following JDBC driver directory:
      <WebSphere installation directory>/lib
3. Create the security account that the Operational Reference Store will use.
   a. Expand Security in the console navigation tree.
   b. Click the Secure administration, applications, and infrastructure link.
   d. Click New, and set the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Name of the Operational Reference Store.</td>
</tr>
<tr>
<td>User ID</td>
<td>User name to connect to the Operational Reference Store.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to access the Operational Reference Store.</td>
</tr>
</tbody>
</table>

e. Click OK.

4. Create the JDBC Provider.
   a. Expand Resources > JDBC, and then click JDBC Providers.

   The JDBC Provider page appears.
Select the scope for applications to use the data source.

Click New, and specify the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database type</td>
<td>Type of database. Select Oracle.</td>
</tr>
<tr>
<td>Provider type</td>
<td>Type of JDBC provider. Select Oracle JDBC Driver.</td>
</tr>
<tr>
<td>Implementation type</td>
<td>Data source implementation type. Select XA data source.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the JDBC provider. Change the name to Informatica MDM Oracle JDBC Provider (XA).</td>
</tr>
</tbody>
</table>

Click Next, and then click Finish.

Create the Operational Reference Store data source.

a. Click the JDBC provider that you created.

The Configuration page appears.

b. Under Additional Properties, click Data sources.

The Data Sources page appears.

c. Click New.

d. Specify the following data source properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Data source name. Specify MDM ODS Data Source.</td>
</tr>
<tr>
<td>JNDI Name</td>
<td>JNDI path to where the JDBC data source will be bound. Specify jdbc/siperian-&lt;Oracle host name&gt;-&lt;Oracle SID&gt;-&lt;Operational Reference Store name&gt;-dsjdbc/siperian-&lt;IBM DB2 host name&gt;-&lt;IBM DB2 database name&gt;-&lt;Operational Reference Store name&gt;-dsjdbc/siperian-&lt;Microsoft SQL Server host name&gt;-&lt;Operational Reference Store name&gt;-ds. <strong>Note:</strong> The JNDI name must be in lower case.</td>
</tr>
<tr>
<td>Component-managed Authentication Alias</td>
<td>Authentication alias of the Master Database data source. Select &lt;host name&gt;/&lt;Operational Reference Store name&gt;.</td>
</tr>
<tr>
<td>Driver Class Name</td>
<td>JDBC driver class. Set to com.microsoft.sqlserver.jdbc.SQLServerXADatasource.</td>
</tr>
</tbody>
</table>

e. Click Next, and then click Finish.

**Configuring WebSphere for Multiple MDM Hub Master Databases**

If you want to configure multiple MDM Hub Master Database instances, configure as many WebSphere profiles as the number of MDM Hub Master Database instances. Each MDM Hub Master Database instance must have its own MDM Hub instance. Therefore, create as many WebSphere profiles to deploy each MDM Hub instance on a separate WebSphere profile.
Configuring the HTTPS Protocol

You can configure the HTTPS protocol for communications between the MDM Hub components such as the Hub Server, Process Server, and ActiveVOS. Configure the HTTPS protocol in the WebSphere application server.

1. Create an SSL-enabled WebSphere port.
2. Configure WebSphere to allow self-signed certificates.

For more information about configuring the HTTPS protocol, see the WebSphere documentation.

Configuring WebSphere for Informatica Data Director

If you want to use Data Director, configure WebSphere and then restart WebSphere for the changes to take effect.

Ensure that you perform the following configurations:

- Set the web container custom property.
  Use the WebSphere Console to set com.ibm.ws.webcontainer.invokeRequestListenerforfilter to true. For instructions on setting web container custom properties, see the WebSphere documentation.

- To support the management of tasks, increase the value for timeout properties by a factor of 2.
  Perform the following task by using the the WebSphere Console:

1. navigate to WebSphere Console Servers > Server Types > WebSphere application servers > <target server name>.
2. In the Container Services category, click Transaction service and increase the values for the timeout properties.
Chapter 5

Hub Store Upgrade

This chapter includes the following topics:

- Hub Store Upgrade Overview, 69
- Clone the Hub Store (Clean Upgrade), 69
- Databases Set to a Non-English Locale, 70
- Upgrading the MDM Hub Master Database inVerbose Mode, 70
- Upgrading the MDM Hub Master Database in Silent Mode, 71
- Upgrading Operational Reference Store Databases inVerbose Mode, 72
- Upgrading Operational Reference Store Databases in Silent Mode, 75
- Confirm that the Upgrade Scripts Ran Successfully, 76

Hub Store Upgrade Overview

The Hub Store is the database that contains the MDM Hub Master Database and one or more Operational Reference Store (ORS) databases. Use the scripts provided in the distribution to upgrade the databases.

If your database environment is set to a non-English locale, ensure that the character set is a Unicode character set before you upgrade the Hub Store. After the upgrade completes successfully, you can select your preferred locale. The locale is stored as a user account preference, rather than at the database level.

Note: Ensure that you do not include spaces in the path to the database directory or folder names. If you specify a path that has spaces in the directory or folder names, the upgrade fails.

Clone the Hub Store (Clean Upgrade)

If you are performing a clean upgrade, ask a DBA to back up and clone the Master Database and the Operational Reference Stores. Copy the cloned databases to the new environment. You upgrade the Master Database and Operational Reference Stores in the new environment.
Databases Set to a Non-English Locale

If the Hub Store database environment is set to a non-English locale, ensure that the database environment uses a Unicode character set before you run the upgrade script. You set the character set using a database environment variable.

The upgrade script translates metadata to English and associates a translation key with the metadata. After the upgrade is successful, each MDM Hub Console user can select any supported locale for the user interface and databases. The locale selection for each user is stored in the Master Database with all user data.

For example, consider an MDM Hub Store that resides in an Oracle database environment in a Korean locale. Before you upgrade, you ensure that the database environment variable `NLS_LANG` is set to `KOREAN_KOREA.AL32UTF8` (Korean Unicode). After the upgrade, you can set your locale to Korean, while someone else can choose a different supported locale.

The following table lists database environment variables that you can use to set the character set:

<table>
<thead>
<tr>
<th>Database</th>
<th>Environment Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>NLS_LANG</td>
</tr>
<tr>
<td>IBM DB2</td>
<td>DB2CODEPAGE</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>SET LANGUAGE clause (for session only)</td>
</tr>
</tbody>
</table>

For more information about database environment variables, see the documentation for your database.

Upgrading the MDM Hub Master Database in Verbose Mode

To upgrade the MDM Hub Master Database, run the upgrade script.

**Note:** If you did not use the Hub Console to make metadata changes, the database upgrade script might fail. If a script fails, contact Informatica Global Customer Support.

1. Open a command prompt.
2. Navigate to the following directory:
   - In UNIX. `<MDM Hub distribution directory>/database/bin`
   - In Windows. `<MDM Hub distribution directory>\database\bin`
3. Run the MDM Hub Master Database upgrade script with the following command:
   - In UNIX. `sip_ant.sh updatemasterdatabase`
   - In Windows. `sip_ant.bat updatemasterdatabase`
4. Answer the prompts.
5. Answer the following prompt if it appears during the Master Database upgrade:

   This upgrade should be performed by a DBA to grant 'create sequence' privileges for the master database. The master database does not have 'create sequence' privileges,
In JBoss environments, restart the application server.

MDM Hub distribution directory

Navigate to the following directory:

/\database/bin

Save a copy of the CMX_SYSTEM upgrade log files to the upgrade documentation directory. There is an

Open a command prompt.

Mode

2.

1.

7.

To upgrade the MDM Hub Master Database in silent mode, run the upgrade script with the appropriate

The upgrade process saves the files to the following location:

• In UNIX.

<MDM Hub installation directory>/server/resources/database/db_changes/<database

name>/Master

• In Windows.

<MDM Hub installation directory>\server\resources\database\db_changes\<database

name>\Master

Upgrading the MDM Hub Master Database in Silent Mode

To upgrade the MDM Hub Master Database in silent mode, run the upgrade script with the appropriate

command for the environment.

Note: To display the silent upgrade process in the command line, set -Dnoprompt to true. To display the only

the start time and end time in the command line, set -Dnoprompt to true -silent.

1. Open a command prompt.

2. Navigate to the following directory:

• UNIX. <MDM Hub distribution directory>/database/bin

• Windows. <MDM Hub distribution directory>\database\bin

3. To upgrade the MDM Hub Master Database in an Oracle environment, run the following command:

UNIX.

sip_ant.sh updatemasterdatabase -Dmaster.tnsname=<TNS name> -
Dmaster.connectiontype=<SID or SERVICE> -Dmaster.server=<host name> -
Dmaster.port=<port> -Dmaster.sid=<SID name> -Dmaster.username=<MDM Hub Master
Database username> -Dmaster.password=<MDM Hub Master Database password>-
Dcmx.username=<administrator username> -Dcmx.password=<administrator password> -
Dcmx.server.masterdatabase.type=ORACLE -Dnoprompt=true

Windows.

sip_ant.bat updatemasterdatabase -Dmaster.tnsname=<TNS name> -
Dmaster.connectiontype=<SID or SERVICE> -Dmaster.server=<host name> -
Dmaster.port=<port> -Dmaster.sid=<SID name> -Dmaster.username=<MDM Hub Master
To upgrade the MDM Hub Master Database in an IBM DB2 environment, run the following command:

**UNIX.**
```
sip_ant.sh updatemasterdatabase -Dmaster.hostname=<host name> -Dmaster.port=<port> -Dmaster.userame=<MDM Hub Master Database username> -Dmaster.password=<MDM Hub Master Database password> -Ddba.username=DBA username> -Ddba.password=DBA password> -Dnoprompt=true
```

**Windows.**
```
sip_ant.bat updatemasterdatabase -Dmaster.hostname=<host name> -Dmaster.port=<port> -Dmaster.userame=<MDM Hub Master Database username> -Dmaster.password=<MDM Hub Master Database password> -Ddba.username=DBA username> -Ddba.password=DBA password> -Dnoprompt=true
```

To upgrade the MDM Hub Master Database in a Microsoft SQL Server environment, run the following command:

**UNIX.**
```
sip_ant.sh updatemasterdatabase -Dmaster.hostname=<host name> -Dmaster.port=<port> -Dmaster.userame=<MDM Hub Master Database username> -Dmaster.password=<MDM Hub Master Database password> -Dcmmx.username=administrat username> -Dcmmx.password=administrator password> -Dcmmx.server.masterdatabase.type=MSSQL -Dmaster.database=<MDM Hub Master Database name> -Dnoprompt=true
```

**Windows.**
```
sip_ant.bat updatemasterdatabase -Dmaster.hostname=<host name> -Dmaster.port=<port> -Dmaster.userame=<MDM Hub Master Database username> -Dmaster.password=<MDM Hub Master Database password> -Dcmmx.username=administrat username> -Dcmmx.password=administrator password> -Dcmmx.server.masterdatabase.type=MSSQL -Dmaster.database=<MDM Hub Master Database name> -Dnoprompt=true
```

### Upgrading Operational Reference Store Databases inVerbose Mode

To upgrade each Operational Reference Store (ORS) database, run an upgrade script. Upgrade the MDM Hub Master Database before you upgrade the ORS databases.

**Note:** If you did not use the Hub Console to make metadata changes, the database upgrade script might fail. If a script fails, contact Informatica Global Customer Support.

1. **Stop the application server.**
2. **Open a command prompt.**
3. **Navigate to the following directory:**
   - On **UNIX.** `<MDM Hub distribution directory>/database/bin`
   - On **Windows.** `<MDM Hub distribution directory>/database/bin`
4. **Run the Operational Reference Store upgrade script with the following command:**
   - **UNIX.** `./sip_ant.sh updatorsdatabase`
5. Answer the prompts.

For Oracle environments, provide the following information:

<table>
<thead>
<tr>
<th>Prompts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter database type (ORACLE, MSSQL, DB2)</td>
<td>Database type. Specify Oracle.</td>
</tr>
<tr>
<td>Enter Oracle Connection Type (service, sid) [service]</td>
<td>Connection type. Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td>SERVICE</td>
</tr>
<tr>
<td></td>
<td>Uses the service name to connect to Oracle.</td>
</tr>
<tr>
<td></td>
<td>SID</td>
</tr>
<tr>
<td></td>
<td>Uses the Oracle System ID to connect to Oracle.</td>
</tr>
<tr>
<td></td>
<td>Default is SERVICE.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database host name [localhost]</td>
<td>Name of the host that is running the database.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database port number. [1521]</td>
<td>Port number that the database listener uses. Default is 1521.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database service name [orcl]</td>
<td>Name of the Oracle service. This prompt is displayed if the selected Oracle connection type is SERVICE.</td>
</tr>
<tr>
<td>Enter Oracle Net connect identifier (TNS Name) [orcl]</td>
<td>Oracle TNS name. Default is orcl.</td>
</tr>
<tr>
<td>Master Database Connect URL: &quot;jdbc:oracle:thin:@//&lt;host_name&gt;:&lt;port&gt;/&lt;service_name&gt;&quot;. Do you want to change the connect URL (y/n) [n]</td>
<td>Connect URL for the Oracle connection type SERVICE. You can type y to change the default connect URL. To use the default connect URL, type n.</td>
</tr>
<tr>
<td>Enter database SID [orcl]</td>
<td>Name of the Oracle System ID. This prompt is displayed if the selected Oracle connection type is SID.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database name [cmx_ors]</td>
<td>Name of the Operational Reference Store database. Default is cmx_ors.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database user password</td>
<td>Password to access the Operational Reference Store.</td>
</tr>
<tr>
<td>Enter the DBA username [sys]</td>
<td>Name of the user with DBA-level permissions.</td>
</tr>
<tr>
<td>Enter the DBA password</td>
<td>Password of the user with DBA-level permissions.</td>
</tr>
<tr>
<td>Enter integer code of ORS Timeline Granularity: Year 5, Month 4, Day 3, Hour 2, Minute 1, Second 0 [3]</td>
<td>Specify timeline units to use.</td>
</tr>
</tbody>
</table>
For IBM DB2 environments, provide the following information:

<table>
<thead>
<tr>
<th>Prompts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter database type (ORACLE, MSSQL, DB2)</td>
<td>Database type. Specify DB2.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database host name [localhost]</td>
<td>Name of the host that is running the database.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database port number [50000]</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td></td>
<td>Default is 50000.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database name [SIP97]</td>
<td>Name of the database. Default is SIP97.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database name [cmx_ors]</td>
<td>Name of the Operational Reference Store database.</td>
</tr>
<tr>
<td></td>
<td>Default is cmx_ors.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database user password</td>
<td>Password to access the Operational Reference</td>
</tr>
<tr>
<td></td>
<td>Store.</td>
</tr>
<tr>
<td>Enter locale name from list: de, en_US, fr, ja, ko, zh_CN. [en_US]</td>
<td>Operating system locale. Default is en_US.</td>
</tr>
<tr>
<td>Enter the DBA username [sys]</td>
<td>Name of the user with DBA-level permissions.</td>
</tr>
<tr>
<td>Enter the DBA password</td>
<td>Password of the user with DBA-level permissions.</td>
</tr>
<tr>
<td>Enter integer code of ORS Timeline Granularity: Year 5, Month 4, Day 3, Hour 2, Minute 1, Second 0 [3]</td>
<td>Specify timeline units to use.</td>
</tr>
</tbody>
</table>

For Microsoft SQL Server environments, provide the following information:

<table>
<thead>
<tr>
<th>Prompts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter database type (ORACLE, MSSQL, DB2)</td>
<td>Database type. Specify MSSQL.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database host name [localhost]</td>
<td>Name of the host that is running the database.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database port number [1433]</td>
<td>Port number that the database listener uses.</td>
</tr>
<tr>
<td></td>
<td>Default is 1433.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database name [cmx_ors]</td>
<td>Name of the Operational Reference Store database.</td>
</tr>
<tr>
<td></td>
<td>Default is cmx_ors.</td>
</tr>
<tr>
<td>Enter the Operational Reference Store database user password</td>
<td>Password to access the Operational Reference</td>
</tr>
<tr>
<td></td>
<td>Store.</td>
</tr>
<tr>
<td>Enter locale name from list: de, en_US, fr, ja, ko, zh_CN. [en_US]</td>
<td>Operating system locale. Default is en_US.</td>
</tr>
<tr>
<td>Enter the DBA username [sys]</td>
<td>Name of the user with DBA-level permissions.</td>
</tr>
</tbody>
</table>
Register the upgraded ORS in the Hub Console.

6. Restart the application server.
7. Save a copy of the CMX_ORS upgrade log files to the upgrade documentation directory. There is a log file for each change script.

The upgrade process saves the files to the following location:

- In UNIX.
  `{<MDM Hub installation directory>/server/resources/database/db_changes/<database name>/ORS`
- In Windows.
  `{<MDM Hub installation directory>/server/resources/database/db_changes/<database name>/ORS`

**Important:** The sip_ant log file is overwritten every time you execute sip_ant from the command line. You must save a backup copy before you run the sip_ant script to upgrade another ORS.

**RELATED TOPICS:**
- “Saving the MDM Hub Environment Report” on page 117

---

**Upgrading Operational Reference Store Databases in Silent Mode**

To upgrade an Operational Reference Store database in silent mode, run the upgrade script with the appropriate command for the environment.

**Note:** To display the silent upgrade process in the command line, set `-Dnoprompt` to `true`. To display the only the start time and end time of the silent upgrade process in the command line, set `-Dnoprompt true silent`.

1. Open a command prompt.
2. Navigate to the following directory:
   - UNIX. `{<MDM Hub distribution directory>/database/bin`
   - Windows. `{<MDM Hub distribution directory>/database/bin`
3. To upgrade an Operational Reference Store in an Oracle environment, run the following command:

   UNIX.
   ```
sip_ant.sh updateorsdatabase -Dors.tnsname=<tns name> -Dors.connectiontype=sid -Dors.hostname=<hostname> -Dors.port=<port> -Dors.sid=<Oracle SID> -Dors.username=<ORS username> -Dors.password=<ORS password> -Dcmx.server.masterdatabase.type=oracle -Dnoprompt=true
   ```

---

### Prompts and Description

<table>
<thead>
<tr>
<th>Prompts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the DBA password</td>
<td>Password of the user with DBA-level permissions.</td>
</tr>
<tr>
<td>Enter integer code of ORS Timeline Granularity: Year 5, Month 4, Day 3, Hour 2, Minute 1, Second 0 [3]</td>
<td>Specify timeline units to use.</td>
</tr>
</tbody>
</table>
Windows.

```
sip_ant.bat updateorsdatabase -Dors.tnsname=<tns name> -Dors.connectiontype=sid -
Dors.hostname=<hostname> -Dors.port=<port> -Dors.sid=<Oracle SID> -
Dors.username=<ORS username> -Dors.password=<ORS password> -
Dcmx.server.masterdatabase.type=oracle -Dnprompt=true
```

4. To upgrade the Operational Reference Store in an IBM DB2 environment, run the following command:

UNIX.

```
sip_ant.sh updateorsdatabase -Dors.hostname=<host name> -Dors.database=%db2database%
-Dors.port=<port>
-Dors.username=<ORS username> -Dors.password=<ORS password>
Dcmx.server.masterdatabase.type=db2 -Dnprompt=true
```

Windows.

```
sip_ant.bat updateorsdatabase -Dors.hostname=<host name> -Dors.database=%db2database%
-Dors.port=<port>
-Dors.username=<ORS username> -Dors.password=<ORS password>
Dcmx.server.masterdatabase.type=db2 -Dnprompt=true
```

5. To upgrade the Operational Reference Store in a Microsoft SQL Server environment, run the following command:

UNIX.

```
sip_ant.sh updateorsdatabase -Dors.hostname=<host name> -Dors.port=<port> -
Dors.username=<ORS username>
-Dors.password=<ORS password> -Dors.database=<database name> -
Dcmx.server.masterdatabase.type=MS SQL
-Dnprompt=true
```

Window.

```
sip_ant.bat updateorsdatabase -Dors.hostname=<host name> -Dors.port=<port> -
Dors.username=<ORS username>
-Dors.password=<ORS password> -Dors.database=<database name> -
Dcmx.server.masterdatabase.type=MS SQL
-Dnprompt=true
```

Confirm that the Upgrade Scripts Ran Successfully

Check the C_REPOS_DB_CHANGE table to see that the Hub Store upgrade scripts ran successfully.

Scripts run during the upgrade process if they have not run during previous upgrades. If the
C_REPOS_DB_CHANGE table indicates that a script failed, contact Informatica Global Customer Support.
Chapter 6

Hub Server Upgrade (In-place Upgrade)

This chapter includes the following topics:

- **Hub Server Upgrade Overview, 77**
- **Upgrading the Hub Server in Graphical Mode, 78**
- **Upgrading the Hub Server in Console Mode, 81**
- **Upgrading the Hub Server in Silent Mode, 83**
- **Run the patchInstallSetup Script, 85**
- **Copy Hub Server Log Files to the Upgrade Documentation Folder, 86**
- **Reapplying the Hub Server Upgrade (Optional), 87**

Hub Server Upgrade Overview

The Hub Server runs the core and common services for MDM, including access, security, and session management. The Hub Server is deployed in an application server environment.

**Note:** This chapter is for an in-place upgrade only. For a clean upgrade, install the Hub Server by following the instructions in the *Multidomain MDM Installation Guide* for your application server and database environment.

You can upgrade the Hub Server in graphical mode, console mode, or silent mode. To upgrade the Hub Server in graphical mode or console mode, run the Hub Server Installer provided in the distribution. To upgrade the Hub Server in silent mode, configure the silent installer properties files.

If you use a version of ActiveVOS Server that is not supported, you are prompted to install ActiveVOS Server during the Hub Server upgrade process.

The Hub Server installer differentiates a patch installation from a full installation when, during installation, you point to the existing MDM Hub installation as the target. Before overwriting the existing Hub Server installation, the MDM Hub Installer creates a backup of critical files.
Upgrading the Hub Server in Graphical Mode

To upgrade the Hub Server in graphical mode, run the Hub Server installer.

**Tip:** If you use embedded ActiveVOS, the upgrade process requires you to install the updated version of ActiveVOS in a new directory. If you prefer to overwrite your existing ActiveVOS installation, before you begin the upgrade, open the ..\hub\server\bin\build.properties file and comment out the following property: `activevos.install.dir = <AVOS installed path>`. For other pre-upgrade tasks, see "Prepare the BPM Upgrade" on page 23.

1. Log in using the user name that was used to install the Hub Server.
2. Start the application server on which the Hub Server is deployed.
3. Open a command prompt and navigate to the Hub Server installer in the distribution directory. By default the installer is in the following directory:
   - On UNIX. `<MDM Hub distribution directory>/<operating system name>/mrmserver`
   - On Windows. `<MDM Hub distribution directory>\windows\mrmserver`
4. Run the following command:
   - On UNIX. `hub_install.bin`
   - On Windows. `hub_install.exe`
5. From the *Introduction* window, click *Next.* The *License Agreement* window appears.
6. Review and accept the terms of the license agreement. Click *Next.*
7. Select the location of the Hub Server installation. The Hub Server installation folder contains the `siperian-mrm.ear` file. Click *Next.* The *Version Warning* message appears.
8. Click *OK* to upgrade an existing Hub Server installation.
9. If the previous installation uses WebLogic as the application server, the Hub Server installer prompts you to provide the WebLogic Admin password. Enter the WebLogic password.
10. If you use, or want to use, ActiveVOS for business process management, install the embedded ActiveVOS version that is recommended for this version of Multidomain MDM.
    **Note:** If you already have a supported version of ActiveVOS installed, you can skip some of the substeps in this step. Perform substep c. to enter database details and substep 12f. to specify the user name and password for the ActiveVOS Server Administration Console.
    a. Select *Yes.*
    b. On the *Choose ActiveVOS Installation Folder* page, accept the default path or select another location. Click *Next.*
    c. On the *Database Information* page, enter the database details that you specified when you created the ActiveVOS database schema, and click *Next.*
      **Note:** If you are moving from standalone ActiveVOS to embedded ActiveVOS, enter the details for the standalone ActiveVOS schema.
    d. On the *Application Server Web URL* page, accept the default URL or specify the URL that you want to use to call ActiveVOS web services. Ensure the URL contains the correct port number for the connection to the application server. Click *Next.*
The post installation setup script uses the URL to call ActiveVOS web services, deploy the predefined MDM workflows to ActiveVOS, and create the URN mapping.

e. On the **ActiveVOS Installer** page, click **Choose**. Browse to the ActiveVOS_Server installation file in the distribution package. Click **Next**.

f. Enter the administrative user name and password to create an administrative user for the ActiveVOS Console.

   **Important:** The user name and password must be the same as the ActiveVOS Console user name and password that was created in the application server.

g. Click **Next**.

11. Select one of the following Informatica platform installation options:

   - **Yes.** Install Informatica platform.
   - **No.** Does not install Informatica platform.

12. If you select **Yes** in the preceding step, click **Choose** and browse to the following Informatica platform file locations:

   - Installation response file
   - Platform installation file

13. On the Product Usage Toolkit page, select the industry to which the organization belongs and the environment type.

14. If you want to use a proxy server, select **Yes**, and enter the proxy server details. Otherwise, select **No**.

   You can enter the following proxy server details:

   - Proxy server name/IP
   - Proxy server port
   - Proxy server domain name. Leave blank if not applicable.
   - Proxy server user name. Leave blank if not applicable.
   - Proxy server password. Leave blank if not applicable.

15. Click **Next**.

   The Deploy window appears.
16. Select whether to deploy the Hub Server EAR file automatically or manually, and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Conditions</th>
</tr>
</thead>
</table>
| Yes, run the script during this installation | Deploys the Hub Server EAR file automatically after a successful installation. Select this option if you use one of the following application server environments:  
  Application server environments:  
  • JBoss standalone environment  
  • WebSphere standalone environment  
  ActiveVOS scenarios:  
  • You chose to install ActiveVOS and no other version of ActiveVOS is installed in this environment.  
  • You chose to install ActiveVOS and the environment includes a supported version of ActiveVOS. Check the product availability matrix (PAM) for supported versions.  
  • You chose not to install ActiveVOS.  
  **Important:** If you chose to install ActiveVOS but you have an unsupported version of ActiveVOS in your environment, select **No, I will run it later**. |
| No, I will run it later                      | You package and deploy the Hub Server EAR file manually. Select this option if you use one of the following application server environments, with or without ActiveVOS:  
  • WebLogic standalone environment  
  • WebLogic clustered environment  
  • JBoss clustered environment  
  • WebSphere clustered environment  
  If you are using any application server environment that includes an unsupported version of ActiveVOS, select this option. You must upgrade the ActiveVOS schema to the supported version and then deploy manually. |

The **Pre-Installation Summary** window appears.

17. To change any options, click the **Previous** button to change your previous selections.

18. After the summary window displays the options you want, click **Install** to start the installation process.

The Hub Server installer displays the **Please Wait** screen while the installer configures the system. The Hub Server installer backs up critical files to an archive that is stored in the **backup** folder in the MDM Hub installation directory. The file name of the archive uses the format shown in the following example:

```
Informatica MDM Hub Server-2010-09-27_12-13.jar
```

When the installation completes, the **Install Complete** window appears.

19. Click **Done** to exit the Hub Server installer.

**Note:** If the upgrade does not complete successfully, a window appears that states that the upgrade failed and displays the location of the log file that contains the failure messages.

20. If you selected **No, I will run it later**, repackage and deploy the Hub Server EAR file.

a. If you have an unsupported version of ActiveVOS in your environment, update the ActiveVOS schema to the supported version.

b. Run the following command to repackage the EAR file:

   **On UNIX.**
   ```
   cd <MDM Hub installation directory>/hub/server/bin
   ./sip_ant.sh repackage
   ```
On Windows.

    cd <MDM Hub installation directory>\hub\server\bin
    sip_ant.bat repackage

c. From the application server administration console, manually deploy the Hub Server EAR file. Refer to the application server documentation.

21. Restart the application server.

Upgrading the Hub Server in Console Mode

You can upgrade the Hub Server in console mode in UNIX.

**Tip:** If you use embedded ActiveVOS for business process management, the upgrade process requires you to install the updated version of ActiveVOS in a new directory. If you prefer to overwrite the existing ActiveVOS installation, before you begin the upgrade, open the ./.hub/server/bin/build.properties file and comment out the following property: activevos.install.dir = <AVOS installed path>.

1. Start the application server.
2. Navigate to the following directory in the MDM Hub distribution:
   On UNIX: <MDM Hub distribution directory>/<operating system name>/mrmsserver
3. Run the following command from the command prompt:
   ./hub_install.bin -i console
4. Enter the number of the locale you want to choose for the upgrade, and then press Enter.
   The introduction information about the upgrade appears.
5. Press Enter.
   The license agreement appears.
6. Read the License Agreement. Type Y to accept the terms of the license agreement, or type N if you do not want to accept the license agreement and want to exit the installation program.
7. Press Enter.
   If you entered Y in the preceding step, information about the installation folder appears.
8. Specify the directory where you installed the Hub Server.
   • To choose the default folder, press Enter.
   • To change the path, type the absolute path of the installation folder, and press Enter.
9. Confirm the location of the installation folder. Type Y to confirm the installation folder, or type N to change the installation folder.
   The version warning message appears.
10. Press Enter to confirm that you want to proceed.
11. In WebLogic environments, enter your WebLogic password, and press Enter.
12. If you use, or want to use, embedded ActiveVOS for business process management, install the embedded ActiveVOS version that is recommended for this version of Multidomain MDM.
Note: If you already have a supported version of ActiveVOS installed, you can skip some of the substeps in this step. Perform substep c. to enter database details and substep 12f. to specify the user name and password for the ActiveVOS Server Administration Console.

a. Press Enter for y=Yes.

b. Specify the location where you want to install the ActiveVOS Server.

c. Enter the database details that you specified when you created the ActiveVOS database schema, and click Next.

Note: If you are moving from standalone ActiveVOS to embedded ActiveVOS, enter the details for the standalone ActiveVOS schema.

d. Specify the URL that you want to use to call MDM and ActiveVOS web services. Ensure the URL contains the correct port number for the connection to the application server.

e. On the ActiveVOS Installer page, select Choose and browse to the ActiveVOS_Server installation file in the distribution package.

f. Enter a user name and password to create an administrative user for the ActiveVOS Server Administration Console.

Important: The user name and password must be the same as the ActiveVOS Console user name and password that was created in the application server.

13. Press Enter.

The Informatica platform installation prompt appears.

14. If you want to install the Informatica platform, press Enter for Yes. Otherwise, type 2 for No and press Enter.

The prompts for the Informatica platform installation response file and archive file locations appear.

15. Enter the locations of the Informatica platform installation response file and archive file, and press Enter.

16. Specify the Product Usage Toolkit options.

a. Enter the industry to which the organization belongs, and then press Enter.

b. Enter the environment type. Type 1 for Production, type 2 for Test/QA, or type 3 for Development, and then press Enter.

17. Select whether you have a proxy server. Press Enter for Yes. Otherwise, type 2 for No and then press Enter.

You can enter the following proxy server details:

- Proxy server name/IP
- Proxy server port
- Proxy server domain name. Leave blank if not applicable.
- Proxy server user name. Leave blank if not applicable.
- Proxy server password. Leave blank if not applicable.

The summary of the installation choices appears.
18. Select whether to deploy the Hub Server EAR file automatically or manually, and then click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Conditions</th>
</tr>
</thead>
</table>
| Yes, run the script during this installation | Deploys the Hub Server EAR file automatically after a successful installation. Select this option if you use one of the following application server environments with one of the ActiveVOS scenarios:  
  Application server environments:  
  - JBoss standalone environment  
  - WebSphere standalone environment  
  ActiveVOS scenarios:  
  - You chose to install ActiveVOS and no other version of ActiveVOS is installed in this environment.  
  - You chose to install ActiveVOS and the environment includes a supported version of ActiveVOS. Check the product availability matrix (PAM) for supported versions.  
  - You chose not to install ActiveVOS.  
  **Important:** If you chose to install ActiveVOS but you have an unsupported version of ActiveVOS in your environment, select **No, I will run it later**. |
| No, I will run it later                      | You package and deploy the Hub Server EAR file manually. Select this option if you use one of the following application server environments, with or without ActiveVOS:  
  - WebLogic standalone environment  
  - WebLogic clustered environment  
  - JBoss clustered environment  
  - WebSphere clustered environment  
  If you are using any application server environment that includes an unsupported version of ActiveVOS, select this option. You must upgrade the ActiveVOS schema to the supported version and then deploy manually. |

The **Pre-Installation Summary** window appears.

19. Press **Enter**.

   The summary of the upgrade choices appears.

20. Verify the information in the pre-upgrade summary. If the information is correct, press **Enter** to start the upgrade. If you need to make changes, type **BACK** to the specific information and make changes.

   When the process is complete, the upgrade completion information appears.

21. Press **Enter** to exit the installer.

---

**Upgrading the Hub Server in Silent Mode**

You can upgrade the Hub Server without user interaction in silent mode. You might want to perform a silent upgrade if you have multiple installations, or if you need to upgrade on a machine cluster. A silent upgrade does not show any progress or failure messages.

Before you run the silent upgrade for the Hub Server, you must configure the properties file for the silent upgrade. The installer reads the file to determine the upgrade options. The silent upgrade process might complete successfully even if you provide incorrect settings, such as an incorrect application server path or port. You must ensure that you provide correct settings in the properties file.
Copy the Hub Server upgrade files to the hard disk on the machine where you plan to install the Hub Server. To upgrade in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the upgrade with the installation properties file.

### Configuring the Properties File

Verify the values of the parameters in the properties file that affect the silent upgrade process.

1. Find the properties file that you configured when you installed the Hub Server.
2. If you are installing the bundled, licensed version of the ActiveVOS Server, add the ActiveVOS properties to your properties file.
   a. Open the `silentInstallServer_sample.properties` file that ships with this release.
   b. Search for `ActiveVOS`.
   c. Copy the `ActiveVOS Installation section to your properties file`.

```
# Multidomain
#
# If you are moving from standalone ActiveVOS to embedded ActiveVOS, enter the
details for the standalone ActiveVOS schema.
```

d. In your properties file, specify the information for your ActiveVOS database and remove the properties for the other supported databases. If you need help with properties, see the *Multidomain MDM Installation Guide* for your environment.
3. If you use the licensed version of ActiveVOS server, add and configure the following properties in the silent installation properties file:

```
SIP.APPSERVER.WEB.URL=http://localhost:8080
# Avos console's administrator username
AVOS CONSOLE.USER=avadmin
# Avos console's administrator password
AVOS.CONSOLE.PASSWORD=admin
# The user name and password must be the same as the ActiveVOS Console user name and password
# that was created in the application server during the pre-installation process.
```

### Running the Silent Upgrade

After you configure the properties file, you can start the silent upgrade.

1. Ensure that the application server is running.
2. Open a command window.
3. Run the following command:
   - On UNIX: `./hub_install.bin -f <location of silent properties file for hub server>`
   - On Windows: `hub_install.exe -f <location of silent properties file for hub server>`

The silent upgrade runs in the background. The process can take a while. If you ran the postInstallSetup script for the Hub Server as part of the silent installation, check the postinstallSetup.log files to verify that the upgrade was successful.

The log file is available in the following directory:
- On UNIX: `<MDM Hub installation directory>/hub/server/logs/
- On Windows: `<MDM Hub installation directory>\hub\server\logs\`

### Run the patchInstallSetup Script

If you chose to deploy manually during the Hub Server installation, you must run the patchInstallSetup script.

1. Navigate to the following directory: `<MDM Hub installation directory>/hub/server`
2. Run the following command to deploy the Hub Server application and apply changes to the application server configuration.
   - **On UNIX**
     - **Note:** On UNIX, if you include an exclamation mark (!) character in the password, you must include a backslash before the exclamation mark (!) character. For example, if the password is `!!cmx!!`, enter `\\!!cmx\\!!`.
     - **WebLogic**
       ```
       patchInstallSetup.sh -Dweblogic.password=<WebLogic password> -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>
       ```
   - **Important:** In a WebLogic 12.2.1.3 or later environment, if you decided to install ActiveVOS or if you decided to use the WebLogic T3S protocol, add the options that match your decisions:
     - ActiveVOS installed. `-Dinstall.avos.patch=true`
• T3S protocol used. -Dweblogic.naming.protocol=t3s

WebSphere with security enabled

patchInstallSetup.sh -Dwebsphere.password=<WebSphere password> -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

WebSphere with security disabled

patchInstallSetup.sh -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

JBoss

patchInstallSetup.sh -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

On Windows

WebLogic

patchInstallSetup.bat -Dweblogic.password=<WebLogic password> -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

Important: In a WebLogic 12.2.1.3 or later environment, if you decided to install ActiveVOS or if you decided to use the WebLogic T3S protocol, add the options that match your decisions:

• ActiveVOS installed. -Dinstall.avos.patch=true

• T3S protocol used. -Dweblogic.naming.protocol=t3s

WebSphere with security enabled

patchInstallSetup.bat -Dwebsphere.password=<WebSphere password> -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

WebSphere with security disabled

patchInstallSetup.bat -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

JBoss

patchInstallSetup.bat -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS Console username> -Davos.password=<ActiveVOS Console password> -Davos.jdbc.database.password=<ActiveVOS database password>

Copy Hub Server Log Files to the Upgrade Documentation Folder

Save a copy of the Hub Server log files. Use these log files assist if you need to troubleshoot the upgrade.

Copy the Hub Server log files to the upgradedoc upgrade documentation folder. Save these files in a separate subfolder, such as hub_server_upgrade. If you upgraded multiple Hub Servers in a cluster, save the files for each Hub Server instance in a separate folder.
The following table describes the log files to copy:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MDM Hub installation directory&gt;/hub/server/Infamdm_Hub_Server_InstallLog.xml</code></td>
<td>Contains log messages for the Hub Server installation.</td>
</tr>
<tr>
<td><code>&lt;MDM Hub installation directory&gt;/hub/server/infamdm_installer_debug.txt</code></td>
<td>Contains debug messages and all the options that you selected when you ran the upgrade process.</td>
</tr>
<tr>
<td><code>&lt;MDM Hub installation directory&gt;/hub/server/logs/patchInstallSetup.log</code></td>
<td>Contains the <code>patchInstallSetup</code> script results.</td>
</tr>
<tr>
<td><code>&lt;MDM Hub installation directory&gt;/hub/server/logs/cmxserver.log</code></td>
<td>Contains the Hub Server log. The Hub Server creates this file when you start the Hub Server.</td>
</tr>
<tr>
<td>Application server log files.</td>
<td>Located in the tree under the installation directory for the application server.</td>
</tr>
</tbody>
</table>

### Reapplying the Hub Server Upgrade (Optional)

If you complete the Hub Server upgrade, the upgrade process does not allow you to reapply the Hub Server upgrade. For example, you might want to reapply the Hub Server upgrade if hardware fails during the upgrade process. You can also perform this procedure if you test an upgrade and then want to revert to an earlier version of the software.

1. **Back up the `siperian-mrm.ear` file in the following directory:**
   - On UNIX: `<MDM Hub installation directory>/hub/server`
   - On Windows: `<MDM Hub installation directory>/hub/server`

2. **Repeat the upgrade steps. Add the parameter `-DSIPERIAN_FORCED_PATCH_INSTALL=true` to the install command.**

   For example, if you reapply the upgrade in graphical mode in UNIX, run the following command:

   ```bash
   hub_install.bin -DSIPERIAN_FORCED_PATCH_INSTALL=true
   ```
Chapter 7

Process Server Upgrade (In-place Upgrade)

This chapter includes the following topics:

- Process Server Upgrade Overview, 88
- Upgrading the Process Server in Graphical Mode, 88
- Upgrading the Process Server in Console Mode, 90
- Upgrading the Process Server in Silent Mode, 92
- Steps to Upgrade to Informatica Address Verification 5 Integration, 93
- Configure Match Population, 95
- Copy Process Server Log Files to the Upgrade Documentation Directory, 97
- Reapplying the Process Server Upgrade (Optional), 98

Process Server Upgrade Overview

The Process Server is a servlet that handles data cleansing operations, match operations, and batch jobs. To upgrade the Process Server, run the Process Server installer provided in the distribution. The Process Server installer differentiates an upgrade from a full installation when you select the existing MDM Hub installation location as the target location during the upgrade process. Before overwriting the existing Process Server installation, the Process Server Installer creates a backup of critical files.

Note: This chapter is for an in-place upgrade only. For a clean upgrade, install the Process Server by following the instructions in the Multidomain MDM Installation Guide for your application server and database environment.

Upgrading the Process Server in Graphical Mode

To upgrade the Process Server in graphical mode, run the Process Server installer.

1. Log in using the user name that was used to install the Process Server.
2. Start the application server on which the Process Server is deployed.
3. Open a command prompt and navigate to the Process Server installer in the distribution directory. By default the installer is in the following directory:
   • On UNIX. <MDM Hub distribution directory><operating system name>/mrmcleanse
   • On Windows. <MDM Hub distribution directory>\windows\mrmcleanse

4. Run the following command:
   • On UNIX. hub_cleanse_install.bin
   • On Windows. hub_cleanse_install.exe

5. From the Introduction window, click Next.
   The License Agreement window appears.

6. Select the I accept the terms of the License Agreement option, and then click Next.
   The Choose Install Folder window appears.

   • To choose the default location, click Next.
   • To choose another location, click Choose, and then click Next.
   The Version Warning message appears.

8. Click OK to confirm that you want to proceed.
   The Enter Location of License File window appears.

9. Select the location of the license file, and then click Next.

10. If the previous installation uses WebLogic as the application server, the Process Server Installer prompts you to provide the WebLogic Admin password. Enter the WebLogic password.

11. On the Product Usage Toolkit page, select the Environment Type.

12. If you have a proxy server, select Yes, and enter the proxy server details. Otherwise, select No, and click Next.
   You can enter the following proxy server details:
   • Proxy server name/IP
   • Proxy server port
   • Proxy server domain name. Leave blank if not applicable.
   • Proxy server user name. Leave blank if not applicable.
   • Proxy server password. Leave blank if not applicable.

13. Click Next.
   The Deploy page appears.

14. Select whether to deploy automatically or manually. click Yes to deploy automatically, or click No to deploy manually, and then click Next.
   • On WebSphere standalone environments or JBoss standalone environments, click Yes to deploy automatically, and then click Next.
   • On WebLogic or clustered environments, click No to deploy manually, and then click Next.
   The Pre-Installation Summary window appears.

15. To change any options, click the Previous button to change your previous selections.

16. After the summary window displays the options you want, click Install to start the installation process.
The Process Server installer displays the Please Wait screen while the installer configures the system. The Process Server installer backs up critical files to an archive that is stored in the backup folder in the MDM Hub installation directory. The file name of the archive uses the format shown in the following example:

Siperian Hub Cleanse Match Server-2010-05-12_18-09.jar

When the installation completes, the Install Complete window appears.

17. **Click Done** to exit the Process Server installer.

**Note:** If the upgrade does not complete successfully, a window appears that states that the upgrade failed and displays the location of the log file that contains the failure messages.

18. If you selected No in step 14, repackage and manually deploy the EAR file.

   a. Run the following command to repackage the EAR file:

      On UNIX.
      ```
      cd <MDM Hub installation directory>/hub/cleanse/bin
      ./sip_ant.sh repackage
      ```

      On Windows.
      ```
      cd <MDM Hub installation directory>/hub\cleanse\bin
      sip_ant.bat repackage
      ```

   b. From the application server administration console, manually deploy the Process Server EAR file. Refer to the application server documentation.

19. Copy the SSA-Name3 library files from `<MDM Hub installation directory>/hub/cleanse/lib/upgrade/SSA` to `<MDM Hub installation directory>/hub/cleanse/lib`.

20. Restart the application server.

---

**Upgrading the Process Server in Console Mode**

You can upgrade the Process Server in console mode on UNIX.

**Note:** Do not use the root user when you upgrade the Process Server on RedHat Linux. The root user does not have a .profile, which InstallAnywhere requires. Instead, create and use a separate user profile to upgrade the Process Server.

1. Start the application server.

2. Navigate to the following directory in the MDM Hub distribution:

   On Solaris. `<MDM Hub distribution directory>/solaris/mrmcleanse`
   
   On HP-UX. `<MDM Hub distribution directory>/hpux/mrmcleanse`
   
   On Linux. `<MDM Hub distribution directory>/linux/mrmcleanse`
   
   On AIX. `<MDM Hub distribution directory>/aix/mrmcleanse`

3. Run the following command from the command prompt:

   ```
   ./hub_cleanse_install.bin -i console
   ```

4. Enter the number of the locale you want to choose for the installation, and then press **Enter**.

   The introduction information about the installation appears.

5. **Press Enter**.

   The license agreement appears.
6. Read the License Agreement. Type **Y** to accept the license agreement, or type **N** if you do not want to accept the license agreement and want to exit the installation program.

7. Press **Enter**.
   
   If you entered **Y** in the preceding step, information about the installation folder appears.

8. Specify the directory where you installed the Process Server.
   - To choose the default location, press **Enter**.
   - To change the path, type the absolute path of the installation folder, and press **Enter**.

9. Confirm the location of the installation folder. Type **Y** to confirm the installation folder, or type **N** to change the installation folder.
   
   The version warning message appears.

10. Press **Enter** to confirm that you want to proceed.
    
    The prompt for the license file location appears.

11. Enter the absolute path of the license file, and press **Enter**.

12. In WebLogic environments, enter your WebLogic password, and press **Enter**.

13. From the Product Usage Toolkit options, select the environment type. Type 1 for Production, type 2 for Test/QA, or type 3 for Development, and then press **Enter**.

14. Select whether you have a proxy server. Press **Enter** for Yes. Otherwise, type 2 for No and then press **Enter**.

   You can enter the following proxy server details:
   - Proxy server name/IP
   - Proxy server port
   - Proxy server domain name. Leave blank if not applicable.
   - Proxy server user name. Leave blank if not applicable.
   - Proxy server password. Leave blank if not applicable.

   The summary of the installation choices appears.

15. Choose whether you want to run the **postInstallSetup** script as part of the installation, or run it manually later.

16. Press **Enter**.

   The summary of the upgrade choices appears.

17. Verify the information in the pre-upgrade summary. If the information is correct, press **Enter** to start the upgrade. If you need to make changes, type **BACK** to the specific information and make changes.

   When the process is complete, the upgrade completion information appears.

18. Press **Enter** to exit the installer.
Upgrading the Process Server in Silent Mode

You can upgrade the Process Server without user interaction in silent mode. You might want to perform a silent upgrade if you have multiple installations, or if you need to upgrade on a machine cluster. A silent upgrade does not show any progress or failure messages.

Before you run the silent upgrade for the Process Server, you must configure the properties file for the silent upgrade. The installer reads the file to determine the upgrade options. The silent upgrade process might complete successfully even if you provide incorrect settings, such as an incorrect application server path or port setting. You must ensure that you provide correct settings in the properties file.

Copy the Process Server upgrade files to the hard disk on the machine where you plan to upgrade the Process Server. To upgrade in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the upgrade with the installation properties file.

Configuring the Properties File

Verify the values of the parameters in the properties file that affect the silent upgrade process.

1. Find the properties file that you configured when you installed the Process Server.
2. Use a text editor to open the file and verify the values of the parameters that affect the silent upgrade process.

The following table describes the upgrade parameters to verify:

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Directory where you installed the Process Server.</td>
</tr>
<tr>
<td></td>
<td>For example, C:\&lt;MDM Hub installation directory&gt;\cleanse.</td>
</tr>
<tr>
<td></td>
<td>You must escape backslash characters in the properties file. Use double backslashes when you specify the installation directory path.</td>
</tr>
<tr>
<td>SIP.APPSERVER.PASSWORD</td>
<td>Password to access WebLogic. For WebLogic environments.</td>
</tr>
<tr>
<td>RUN_DEPLOYMENT_FLAG</td>
<td>Runs the postInstallSetup script as part of the silent upgrade. Set to 1 if you want to run postinstallsetup at the end of the silent upgrade. Set to 0 if you do not want to run postinstallsetup.</td>
</tr>
</tbody>
</table>

3. Add and configure the following product usage toolkit properties to the silent installation properties file:

```bash
#Product Usage Toolkit Installation
#CSM_TYPE is the type of Product Usage Toolkit installation. Should not be blank.
CSM_TYPE=Production

# If the network has a proxy server, fill in the following parameters (leave empty if no proxy):
# proxy server host
CSM_HOST=
# proxy server port
CSM_PORT=
# Proxy server domain name (leave blank, if not applicable)
CSM_DOMAIN=
# Proxy server user name (leave blank, if not applicable)
CSM_PROXY_USER_NAME=
#Proxy server password (leave blank, if not applicable)
CSM_PROXY_PASSWORD=
```
Running the Process Server Silent Upgrade

After you configure the properties file, you can start the silent upgrade.

1. Ensure that the application server is running.
2. Open a command window.
3. Run the following command:
   - **On UNIX**: 
     ```bash
     ./hub_cleanse_install.bin -f <location of silent properties file for process server>
     ```
   - **On Windows**: 
     ```bash
     hub_cleanse_install.exe -f <location of silent properties file for process server>
     ```

   The silent upgrade runs in the background. The process can take a while. If you ran the post install script for the Process Server as part of the silent installation, check the postinstallSetup.log files to verify that the upgrade was successful.

   The log file is available in the following directory:
   - **On UNIX**: `<MDM Hub installation directory>/hub/cleanse/logs/`
   - **On Windows**: `<MDM Hub installation directory>\hub\cleanse\logs\`

Steps to Upgrade to Informatica Address Verification 5 Integration

This section describes the upgrade process required for the MDM Hub implementation to use Informatica Address Verification 5.

**Note:** This section is applicable to users with a license for using Informatica Address Verification.

You must perform the following steps to upgrade to Informatica Address Verification 5 integration:

1. **Open the cmxcleanse.properties file.** This file is located at:
   - **Windows**: `<infamdm_install_directory>\hub\cleanse\resources`
   - **UNIX**: `<infamdm_install_directory>/hub/cleanse/resources`

2. **Ensure that the following Informatica Address Verification 5 properties are set in the cmxcleanse.properties files:**
   - **Windows**:
     ```
     cleanse.library.addressDoctor.property.SetConfigFile=C:\infamdm\hub\cleanse\resources\AddressDoctor\5\SetConfig.xml
     cleanse.library.addressDoctor.property.ParametersFile=C:\infamdm\hub\cleanse\resources\AddressDoctor\5\Parameters.xml
     cleanse.library.addressDoctor.property.DefaultCorrectionType=PARAMETERS_DEFAULT
     ```
   - **UNIX**:
     ```
     cleanse.library.addressDoctor.property.SetConfigFile=/u1/infamdm/hub/cleanse/resources/AddressDoctor/5/SetConfig.xml
     cleanse.library.addressDoctor.property.ParametersFile=/u1/infamdm/hub/cleanse/resources/AddressDoctor/5/Parameters.xml
     cleanse.library.addressDoctor.property.DefaultCorrectionType=PARAMETERS_DEFAULT
     ```

3. Save and close the properties file.
4. Copy `SetConfig.xml` and `Parameters.xml` to the location specified in the `cmxcleanse.properties` file.

The following is a sample `SetConfig.xml` file:

```xml
<!DOCTYPE SetConfig SYSTEM 'SetConfig.dtd'>
<SetConfig>
  <General WriteXMLEncoding="UTF-16" WriteXMLBOM="NEVER"
    MaxMemoryUsageMB="600" MaxAddressObjectCount="10" MaxThreadCount="10" />
  <UnlockCode>79FY19AXAS0KLItDC6PAQVVC3KM14F2C</UnlockCode>
  <DataBase CountryISO3="ALL" Type="BATCH_INTERACTIVE" Path="c:\addressdoctor\5"
    PreloadingType="NONE" />
  <DataBase CountryISO3="ALL" Type="FASTCOMPLETION" Path="c:\addressdoctor\5"
    PreloadingType="NONE" />
  <DataBase CountryISO3="ALL" Type="CERTIFIED" Path="c:\addressdoctor\5"
    PreloadingType="NONE" />
  <DataBase CountryISO3="ALL" Type="GEOCODING" Path="c:\addressdoctor\5"
    PreloadingType="NONE" />
  <DataBase CountryISO3="ALL" Type="SUPPLEMENTARY" Path="c:\addressdoctor\5"
    PreloadingType="NONE" />
</SetConfig>

The following is a sample `Parameters.xml` file:

```xml
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE Parameters SYSTEM 'Parameters.dtd'>
<Parameters>
  <WriteXMLEncoding="UTF-16"
    WriteXMLBOM="NEVER" />
  <Process Mode="BATCH"
    EnrichmentGeoCoding="ON"
    EnrichmentCASS="ON"
    EnrichmentSERP="ON"
    EnrichmentSNA="ON"
    EnrichmentSupplementaryGB="ON"
    EnrichmentSupplementaryUS="ON" />
  <Input Encoding="UTF-16"
    FormatType="ALL"
    FormatWithCountry="ON"
    FormatDelimiter="PIPE" />
  <Result AddressElements="STANDARD"
    Encoding="UTF-16"
    CountryType="NAME_EN"
    FormatDelimiter="PIPE" />
</Parameters>
```

5. Specify the Informatica Address Verification 5 unlock code in the configuration file, `SetConfig.xml`.

For more information about the `SetConfig.xml` file and `Parameters.xml` file, refer to your Informatica Address Verification 5 documentation.

6. Copy the Informatica Address Verification 5 library from the following location:

   **Windows:** `<infadm_install_directory>\hub\cleanse\lib\upgrade\AddressDoctor`

   **UNIX:** `<infadm_install_directory>/hub/cleanse/lib/upgrade/AddressDoctor`

7. Replace `JADE.dll` (or equivalent Informatica Address Verification 4 library) with the Informatica Address Verification 5 library at the following location:

   **Windows:** `<infadm_install_directory>\hub\cleanse\lib`

   **UNIX:** `<infadm_install_directory>/hub/cleanse/lib`
For more information, refer to the `libupdate_readme.txt` document available at:

Windows: `<infamdm_install_directory>\hub\cleanse\lib\upgrade`

UNIX: `<infamdm_install_directory>/hub/cleanse/lib/upgrade`

8. Restart the application server.
   Ensure that you are logged in with the same user name that is currently running the application server and that no exceptions occur while starting the application server.

   During the Process Server initialization, you should see a message similar to the following in the terminal console:
   
   `[INFO ] com.siperian.mrm.cleanse.addressDoctor.Library: Initializing AddressDoctor`

10. Start the Cleanse Functions tool.

11. Obtain a write lock (Write Lock > Acquire Lock).

12. Select the Informatica Address Verification cleanse function.

13. Click the Refresh button.

   The Informatica Address Verification 5 cleanse function is added to the Informatica Address Verification cleanse functions node.

Configure Match Population

The match population contains the standard population set to use for the match process. Each supported country, language, or population has a standard population set. You must enable the match population to use for the match rules.

The match population is available as a `population.ysp` file with the Informatica MDM Hub installation. The population name is the same as the ysp file name. If you add a Japanese population, and want to use the Person_Name_Kanji match field, add _Kanji to the population name. For example, Japan_Kanji or Japan_I_Kanji. If you do this, the standard Person_Name match field is not available.

The population that you use must be compatible with the SSA-Name3 version of the MDM Hub. If you need additional population files or if you need an updated population file to upgrade to a later version, contact Informatica Global Customer Support. The first population file that you request with the product is free. You might need population files for other countries or you might need an updated population file to upgrade to a later version of the MDM Hub.

Upgrading custom population files

During the upgrade process, the population files are upgraded. If you have customized your population files, contact Informatica Global Customer Support to have the customizations applied to the upgraded properties file.

Enabling Match Population

You must enable the match population to use for the match rules.

1. Copy the `<population>.ysp` files to the following location:

   On UNIX: `<MDM Hub installation directory>/hub/cleanse/resources/match`
   
   On Windows: `<MDM Hub installation directory>\hub\cleanse\resources\match`
2. In the C_REPOS_SSA_POPULATION metadata table, verify that the population is registered. The seed database for the MDM Hub installation has some populations registered in the C_REPOS_SSA_POPULATION table, but not enabled.

3. If the C_REPOS_SSA_POPULATION table does not contain the population, add it to the table and enable it.

The population name is the same as the ysp file name. For example, if the ysp file name is US.ysp, the population name is US.

To add the population to an Operational Reference Store, use the following steps:

On IBM DB2 or Oracle:

a. Connect to the Operational Reference Store schema that you want to add the population to.

b. In SQL*Plus, run the `add_std_ssa_population.sql` script in the following directory:

   On UNIX: `<MDM Hub installation directory>/server/resources/database/custom_scripts/oracle`

   On Windows: `<MDM Hub installation directory>\server\resources\database\custom_scripts\oracle`

c. Answer the prompts described in the following table:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the population to add</td>
<td>Name of the population.</td>
</tr>
<tr>
<td>Enter a value for ROWID_SSA_POP (example: INFA.0001) DEFAULT [INFA.0001]</td>
<td>Unique value for the ROWID_SSA_POP column of the C_REPOS_SSA_POPULATION metadata table. Default is INFA.0001</td>
</tr>
</tbody>
</table>

The population is registered in the C_REPOS_SSA_POPULATION table.

d. Run the following command to enable the population:

   ```sql
   UPDATE c_repos_ssa_population SET enabled_ind = 1 WHERE population_name = '<Your Population> ';
   COMMIT;
   ```

On Microsoft SQL Server:

a. Run the `add_std_ssa_population.bat` script in the following directory:

   `<MDM Hub installation directory>\server\resources\database\custom_scripts\MSSQL`

b. Answer the prompts described in the following table:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname with MSSQL instance for CMX_ORS DB ('localhost')</td>
<td>Host name of the Microsoft SQL Server instance.</td>
</tr>
<tr>
<td>cmx_ors user name ('cmx_ors')</td>
<td>User name of the Operational Reference Store.</td>
</tr>
<tr>
<td>cmx_ors user password</td>
<td>Password of the Operational Reference Store.</td>
</tr>
</tbody>
</table>
Copy Process Server Log Files to the Upgrade Documentation Directory

Save a copy of the Hub Server log files. Use these log files assist if you need to troubleshoot the upgrade.

Copy the Process Server log files to the upgrade documentation folder. Save these files in a separate subfolder, such as cleanse_match_server_upgrade. If you upgraded multiple Process Servers in a cluster, save the files for each Process Server instance in a separate folder.

The following table describes the log files to copy:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cleanse installation directory&gt;/hub/cleanse/infamdm_installer_debug.txt</td>
<td>Contains debug messages and all the options that you selected when you ran the upgrade process.</td>
</tr>
<tr>
<td>&lt;cleanse installation directory&gt;/hub/cleanse/logs/patchInstallSetup.log</td>
<td>Contains the patchInstallSetup script results.</td>
</tr>
<tr>
<td>&lt;cleanse installation directory&gt;/hub/cleanse/logs/cmserver.log</td>
<td>Contains the Process Server logs.</td>
</tr>
<tr>
<td>Application server log files.</td>
<td>Located in the tree under the installation directory for the application server.</td>
</tr>
</tbody>
</table>
Reapplying the Process Server Upgrade (Optional)

If you complete the Process Server upgrade, the upgrade process does not allow you to reapply the Process Server upgrade. For example, you might want to reapply the Process Server upgrade if hardware fails during the upgrade process. You can also perform this procedure if you test an upgrade and then want to revert to an earlier version of the software.

1. Back up the siperian-mrm.ear file in the following directory:
   - On UNIX. `<MDM Hub installation directory>/hub/cleanse`
   - On Windows. `<MDM Hub installation directory>\hub\cleanse`

2. Repeat the upgrade steps. Add the parameter `-DSIPERIAN_FORCED_PATCH_INSTALL=true` to the `install` command.

   For example, if you reapply the upgrade in graphical mode in UNIX, run the following command:

   ```
   hub_cleanse_install.bin -DSIPERIAN_FORCED_PATCH_INSTALL=true
   ```
This chapter includes the following topics:

- Resource Kit Upgrade Overview, 99
- Uninstalling the Resource Kit (In-place Upgrade), 99
- Installing the Resource Kit, 100

Resource Kit Upgrade Overview

To upgrade to the current version of the Resource Kit, perform a full installation of the Resource Kit. You cannot perform a patch installation of the Resource Kit.

1. If you are performing an in-place upgrade, uninstall the Resource Kit.
2. Install the current version of the Resource Kit.

Uninstalling the Resource Kit (In-place Upgrade)

To remove the installed version of the Resource Kit, you must run the uninstaller. The uninstaller is located in the Resource Kit directory.

1. Start the application server.
2. Open a command prompt and navigate to the following directory:
   - On UNIX, `<Resource Kit installation directory>/deploy/UninstallerData`
   - On Windows, `<Resource Kit installation directory>\deploy\UninstallerData`
3. Run the following command:
   - On UNIX, `Uninstall_Informatica_MDM_Hub_Resource_Kit.bin`
   - On Windows, `Uninstall Informatica MDM Hub Resource Kit.exe`
4. Click **Uninstall**.
   - The **Uninstall Complete** window appears.
5. Uninstall the previous version of the Resource Kit.

6. Click Done.

Installing the Resource Kit

After you uninstall the Resource Kit, install the current version of the Resource Kit.

1. Start the application server.

2. Navigate to the Resource Kit installer in the distribution directory. By default the installer is in the following directory:

   On UNIX. `<MDM Hub distribution directory>/<operating system name>/mrmresourcekit`

   On Windows. `<MDM Hub distribution directory>windows\mrmresourcekit`

3. Run the following command:

   On UNIX. `hub_resourcekit_install.bin`

   On Windows. `hub_resourcekit_install.exe`

4. Select the language for the installation, and then click OK.

   The Introduction window appears.

5. Click Next.

   The License Agreement window appears.

6. Select the I accept the terms of the License Agreement option, and then click Next.

   The Installation Feature window appears.

7. Select the Resource Kit features that you want to install and click Next.

   You can choose the following Resource Kit features:

   **Sample Schema**
   
   Select this option to install the Sample Schema. You must create a sample schema and register it with the Hub Server before you install the sample applications.

   **Samples and Utilities**
   
   Select this option to install the sample applications and utilities. The list of sample applications deployed is stored in the `build.properties` file.

   The `build.properties` file is located in the following directory: `<MDM Hub installation directory>\hub\resourcekit\samples`

   **SIF SDK and Javadocs**
   
   Select this option to install the javadocs, libraries, and resources associated with the SIF SDK.

   **BPM SDK**
   
   Select this option to install the resources associated with the BPM SDK.

   **Jaspersoft**
   
   Select this option to copy the Jaspersoft installer to the Resource Kit home.

   **SSA-NAME3**
   
   Select this option to copy the SSA-NAME3 installer to the Resource Kit home.

   The Choose Install Folder window appears.
8. Select the location of the Resource Kit installation.
   - To choose the default location, click Next.
   - To enter a path, type the path to the installation folder, and click Next.
     Note: The installation fails if you specify a path that has spaces in a folder name.
   - To return to the default installation location, click Restore Default Folder.
   - To choose another location, click Choose, and then click Next.

On UNIX, the Choose Link Folder window appears. On Windows, the Choose Shortcut Folder window appears.

9. Select the location to create a product icon or link, or select the option not to create a product icon or link, and click Next.

   The Configuration Selection window appears.

10. Select a configuration option, and click Next.

   You can choose the following configuration options:

   **Configure Samples**
   Configures the samples.
   
   **Source Only**
   Installs the sources of samples.

   If you select Configure samples, the Resource Kit App Server window appears. If you select Source only, the Pre-Installation Summary window appears.

11. From the Resource Kit App Server window, select the application server on which you want to install the Resource Kit, and click Next.

   The Application Server Home window for the application server that you select appears.

12. Configure the application server settings.

   - Configure the JBoss settings:
     1. Specify the application server installation directory, and then click Next.
        The JBoss Application Server Configuration Name window appears.
     2. Specify the Configuration Name, and then click Next.
        The default value is standalone.
     3. Specify the remote port.

   - Configure the WebLogic settings:
     1. Choose a path to the WebLogic domain installation directory for the domain you want to use for the MDM Hub, and click Next.
        The WebLogic Application Server Login window appears.
2. Enter WebLogic Server login information.
   You can configure the following login parameters:
   
   **Host**
   Name of the host computer that has the WebLogic installation.
   
   **Server**
   Name of the WebLogic Server instance in the domain on which WebLogic is deployed.
   
   **User Name**
   Name of the user for the WebLogic installation.
   
   **Password**
   Password that corresponds to the WebLogic user.
   
   **Port Number**
   Port number on which the WebLogic Server is listening.

- Configure the WebSphere settings:
  1. Choose a path to the WebSphere application server, and click **Next**.
     The **Reminder** window appears.
  2. Ensure that you have fulfilled the prerequisites and click **OK**.
     The **WebSphere Security Selection** window appears.
  3. Select whether WebSphere is security enabled or not, and click **Next**.
     If you select **No**, and then click **Next**, the **WebSphere Application Server Port** window appears.
     Default is **No**.
     Set the server name, and the RMI and SOAP ports for the WebSphere application server. In a clustered environment, enter one of the cluster server names and its corresponding SOAP and RMI port information.
     If you select **Yes**, and then click **Next**, the **WebSphere Application Server Port and User Credentials** window appears. Specify the WebSphere user name and the WebSphere password.

The **Informatica MDM Hub Server** window appears.

13. Enter the information for the Hub Server installation, and click **Next**.
    You can specify the following Hub Server information:
    
    **Server Name**
    Name of the server that hosts the Hub Server.
    
    **Server HTTP Port**
    Port number of the Hub Server.
    
    **Informatica MDM Administrative password**
    Password to access the MDM Hub.

    The **Resource Kit ORS ID** window appears.

14. Select a Resource Kit ORS ID from the list, and click **Next**.
    The list contains the Operational Reference Store IDs that you created. Select an Operational Reference Store ID related to the Sample Schema.
    If you did not register the sample schema, the Operational Reference Store ID for the Sample schema does not appear. Register the sample Operational Reference Store, and then restart the installation.

The **Deployment Selection** window appears.
15. Select a deployment option, and then click **Next**.
   You can select one of the following deployment options:
   **Yes, run it during this installation.**
   Deploys and configures the Resource Kit during the installation.
   **No, it can be deployed later.**
   Select this option to deploy and configure manually at a later time.
   If you chose to install the Samples and Utilities feature, deploy and configure the Resource Kit in this installation step. If you do not deploy and configure the Resource Kit in this installation step, you cannot make changes and redeploy the samples using the postInstallSetup script.
   If you choose to run the post-install setup manually, you cannot deploy the EAR file using the postInstallSetup script at a later time. You must manually edit the EAR file and deploy it to make any changes to your installation.

   The **Pre-Installation Summary** window appears.

16. Review the pre-installation summary to confirm your installation choices, and then click **Install**.
   When the installation completes, the **Install Complete** window appears.

17. Click **Done** to exit the Resource Kit installer.
Post-Upgrade Tasks

This chapter includes the following topics:

- Post-Upgrade Tasks, 104
- Update Properties, 105
- JBoss Post-Upgrade Tasks, 105
- Restart the MDM Hub Environment, 105
- Perform Post-Upgrade Tasks for In-place Upgrade, 106
- Drop Objects, Columns, and References to Deprecated Objects, 106
- Run the PostInstall Script for Deploying the Hub Server (Conditional), 107
- Configure WebSphere Administrative Security, 108
- Configure Cleanse Functions for Platform Transformations, 115
- Validate the Upgraded Metadata, 115
- Review the MDM Hub Environment Report, 117
- Upgrading the SiperianClient Library Classes for the EJB Protocol, 118
- Prepare the MDM Hub Metadata, 118
- Upgrade Tests, 118
- Data Director and Hub Server Properties, 120
- Data Director Global Properties, 121
- Generate the Business Entity Schema, 122

Post-Upgrade Tasks

Whether you perform a clean upgrade or an in-place upgrade, perform the post-upgrade tasks to ensure your environment is properly configured.
**Update Properties**

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update the Application Server Settings in the Properties Files</td>
<td>If you upgrade the application server, you must manually update the application server settings in the properties files.</td>
</tr>
<tr>
<td></td>
<td>In the <code>build.properties</code> file located in <code>&lt;MDM Hub installation directory&gt;\hub\server\bin</code>, update the following settings:</td>
</tr>
<tr>
<td></td>
<td>- SIP.AS.HOME</td>
</tr>
<tr>
<td></td>
<td>- SIP.AS.SERVER_FOLDER</td>
</tr>
<tr>
<td></td>
<td>- SIP.AS.DEPLOY_FOLDER</td>
</tr>
<tr>
<td></td>
<td>In the <code>setSipervisorEnv.bat</code> file located in <code>&lt;MDM Hub installation directory&gt;\hub\server\bin</code>, update the following settings:</td>
</tr>
<tr>
<td></td>
<td>- SET JBS_HOME</td>
</tr>
<tr>
<td></td>
<td>- SET JBS_SERVER_DIR</td>
</tr>
<tr>
<td></td>
<td>- SET JBS_DEPLOY_DIR</td>
</tr>
<tr>
<td></td>
<td>- SET JBS_CLIENT_CLASSPATH</td>
</tr>
<tr>
<td></td>
<td>In the <code>cmxserver.properties</code> file located in <code>&lt;MDM Hub installation directory&gt;\hub\server\resources</code>, update the following settings:</td>
</tr>
<tr>
<td></td>
<td>- cmx.appserver.version</td>
</tr>
<tr>
<td></td>
<td>If you have changed any other application server configuration settings, such as port numbers, you must also update the settings in <code>cmxserver.properties</code>.</td>
</tr>
</tbody>
</table>

**JBoss Post-Upgrade Tasks**

In JBoss environments, perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove the <code>ojdbc6.jar</code> file</td>
<td>Remove the JAR file from the following locations:</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;JBoss install location&gt;\modules\com\activevso\main</code></td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;JBoss install location&gt;\modules\com\informatica\mdm\jdbc\main</code></td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;MDM Hub installation directory&gt;\hub\server\lib</code></td>
</tr>
<tr>
<td>Optionally, update the JDBC driver to <code>sqljdbc42.jar</code></td>
<td>1. Install the JDBC driver as a core module. For instructions, see the JBoss documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Update the <code>datasource definitions</code> in the JBoss standalone-full.xml file to use the module.</td>
</tr>
</tbody>
</table>

**Restart the MDM Hub Environment**

Restart the MDM Hub environment after you upgrade.
Restarting the Application Servers

Restart the application servers and then launch the Hub Console.

1. Shut down the application servers that run the Hub Server and the Process Servers.
2. Start the application servers that run the Hub Server and the Process Servers.

Perform Post-Upgrade Tasks for In-place Upgrade

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear the Java cache</td>
<td>1. Clear the Java WebStart cache. For instructions, see the Java documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Clear the Java cache. For instructions, see the Java documentation.</td>
</tr>
<tr>
<td></td>
<td>3. Launch the Hub Console.</td>
</tr>
<tr>
<td>Delete the ZooKeeper data directory</td>
<td>If you use search, delete the ZooKeeper data directory.</td>
</tr>
<tr>
<td></td>
<td>You set the ZooKeeper data directory when you configure a Process Server as a ZooKeeper Server.</td>
</tr>
</tbody>
</table>

Drop Objects, Columns, and References to Deprecated Objects

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update references to REL_START_DATE, REL_END_DATE, and HUID tables</td>
<td>Update references to the REL_START_DATE and REL_END_DATE system columns and to the HUID table. The upgrade process removes references to the REL_START_DATE and REL_END_DATE columns in the packages and views used in a Hierarchy Manager base object. Change references from REL_START_DATE to PERIOD_START_DATE. Change references from REL_END_DATE to PERIOD_END_DATE.</td>
</tr>
</tbody>
</table>
Run the PostInstall Script for Deploying the Hub Server (Conditional)

If you skipped the `postInstallSetup` script during the installation, run the script. The post-installation process deploys the Hub Server applications, creates data sources, and configures JMS message queues.

If you use a WebLogic Server environment with Managed Servers where the Administration Server and the Managed Servers are on different machines, copy all the deployment files to the MDM Hub installation directory of the Administration Server. For more information, see the *Multidomain MDM Installation Guide*.

- Open a command prompt and run the `postInstallSetup` script the following directory: `<MDM Hub installation directory>/hub/server`

  **Note:** If you did not install the ActiveVOS version that is bundled with the MDM Hub installer, do not include the ActiveVOS user names and passwords in the command. On UNIX, if you include the exclamation mark (!) in your password, you must include a backslash before the exclamation mark. For example, if your password is `!!cmx!!`, enter the following password: `\!!cmx!!`

  **For WebSphere with security disabled:**
  ```
  ./postInstallSetup.sh -dDatabase.password=<MDM Hub Master database password>
  -dAvos.username=<ActiveVOS Console username>
  -dAvos.password=<ActiveVOS Console password>
  -dAvos.jdbc.database.username=<ActiveVOS database username>
  -dAvos.jdbc.database.password=<ActiveVOS database password>
  ```

  **For WebSphere with security-enabled:**
  ```
  ./postInstallSetup.sh -dwebSphere.password=<WebSphere password>
  -dDatabase.password=<MDM Hub Master database password>
  -dAvos.username=<ActiveVOS Console username>
  -dAvos.password=<ActiveVOS Console password>
  -dAvos.jdbc.database.username=<ActiveVOS database username>
  -dAvos.jdbc.database.password=<ActiveVOS database password>
  ```

  **For JBoss:**
  ```
  ./postInstallSetup.sh -ddatabase.password=<MDM Hub Master database password>
  -dAvos.username=<ActiveVOS Console username>
  -dAvos.password=<ActiveVOS Console password>
  -dAvos.jdbc.database.username=<ActiveVOS database username>
  -dAvos.jdbc.database.password=<ActiveVOS database password>
  ```

  **For WebLogic:**
  ```
  ./postInstallSetup.sh -dweblogic.password=<WebLogic password>
  -dDatabase.password=<MDM Hub Master database password>
  -dAvos.username=<ActiveVOS Console username>
  -dAvos.password=<ActiveVOS Console password>
  -dAvos.jdbc.database.username=<ActiveVOS database username>
  -dAvos.jdbc.database.password=<ActiveVOS database password>
  ```

  **Important:** In a WebLogic 12.2.1.3 or later environment, if you decided to install ActiveVOS or if you decided to use the WebLogic T3S protocol, add the options that match your decisions:

  - **ActiveVOS installed.** `-Dinstall.avos.patch=true`
  - **T3S protocol used.** `-Dweblogic.naming.protocol=t3s`

  The ActiveVOS Console credentials are the same credentials as the administrative user in the application server.

  The ActiveVOS database credentials are the same credentials that were used to run the `create_bpm` script.

  If you deploy in a WebLogic environment with Managed Servers, ensure that you specify all the Managed Servers as the targets for deployments in the WebLogic Server Administration Console.

  For more information, see the *Multidomain MDM Installation Guide* and the WebLogic documentation.
Configure WebSphere Administrative Security

You can configure WebSphere administrative security to control MDM Hub access to the WebSphere administrative console.

To configure WebSphere administrative security, perform the following steps:

1. Unregister the Operational Reference Stores (ORS).
2. Uninstall the EAR files and remove data sources from WebSphere.
3. Enable WebSphere administrative security in the WebSphere administrative console.
5. Run the Hub Server and Process Server PostInstallSetup scripts.
6. Register the ORS.

Enter your WebSphere credentials when you register the ORS. You do not need to enter your credentials after you verify the ORS.

Unregister the Operational Reference Store

To unregister the Operational Reference Store (ORS), use the Databases tool in the MDM Hub Console.

1. From the MDM Hub Console, click **Write Lock > Acquire Lock**.
2. From the **Configuration** workbench, select the **Databases** tool.
   
   The **Database Information** page appears.

3. From the list of databases, select the ORS to unregister.
4. Click **Unregister database**.
   
   The Database tool prompts you to confirm that you want to unregister the ORS.

5. Click **Yes**.

Uninstall the EAR files and Remove Data Sources

To uninstall the EAR files and remove data sources, use the WebSphere administrative console.

1. Use the WebSphere administrative console to undeploy the following deployment files:

<table>
<thead>
<tr>
<th>Deployment File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>siperian-mrm.ear</td>
<td>Required. The Hub Server application.</td>
</tr>
<tr>
<td>provisioning-ear.ear</td>
<td>Required. The Provisioning tool application.</td>
</tr>
<tr>
<td>entity360view-ear.ear</td>
<td>Optional. The Entity 360 framework.</td>
</tr>
<tr>
<td>informatica-mdm-platform-ear.ear</td>
<td>Optional. The Informatica platform application.</td>
</tr>
</tbody>
</table>

2. Use the WebSphere administrative console to remove all data sources for the MDM Hub Master Database and the Operational Reference Stores.

3. Restart the application server.

For more information, see the WebSphere documentation.
Enable WebSphere Administrative Security in the WebSphere Administrative Console

You must enable WebSphere administrative security in the WebSphere administrative console. When you enable WebSphere administrative security, disable WebSphere application security.

For more information, see the WebSphere documentation.

Configure the Hub Server and Process Server Properties

You must configure the Hub Server and Process Server property files to enable WebSphere administrative security.

1. Stop the application server.
2. Enable WebSphere security on the Hub Server.
   a. Open cmxserver.properties in the following directory:
      On UNIX. `<MDM Hub installation directory>/hub/server/resources`
      On Windows. `<MDM Hub installation directory>\hub\server\resources`
   b. Set `cmx.websphere.security.enabled` to true.
   a. Open cmxcleanse.properties in the following directory:
      On UNIX. `<MDM Hub installation directory>/hub/cleanse/resources`
      On Windows. `<MDM Hub installation directory>\hub\cleanse\resources`
   b. Set `cmx.websphere.security.enabled` to true.
4. Configure the WebSphere user name on the Hub Server.
   a. Open build.properties in the following directory:
      On UNIX. `<MDM Hub installation directory>/hub/server/bin`
      On Windows. `<MDM Hub installation directory>\hub\server\bin`
   b. Set `websphere.username` to the WebSphere administrative user name.
5. Configure the WebSphere user name on the Process Server.
   a. Open build.properties in the following directory:
      On UNIX. `<MDM Hub installation directory>/hub/cleanse/bin`
      On Windows. `<MDM Hub installation directory>\hub\cleanse\bin`
   b. Set `websphere.username` to the WebSphere administrative user name.
6. In SQL* Plus, run the following command to set \c_repos_cleanse_match_server.is_secured to 1.

   ```sql
   UPDATE c_repos_cleanse_match_server SET is_secured = 1 where rowid_cleanse_match_server="<Insert value here>";
   COMMIT;
   ```
7. Start the application server.

Run the Hub Server PostInstallSetup Script Manually

You must run the Hub Server PostInstallSetup script.

1. Open a command prompt.
2. Navigate to the PostInstallSetup script in the following directory:
   On UNIX. <MDM Hub installation directory>/hub/server
   On Windows. <MDM Hub installation directory>\hub\server
3. Run the following command:
   On UNIX. postinstallsetup.sh -database.password=<MDM Hub Master Database> -DwebspHERE.password=<WebSphere administrative user password>
   On Windows. postinstallsetup.bat -database.password=<MDM Hub Master Database> -DwebspHERE.password=<WebSphere administrative user password>
4. Restart the application server.

Run the Process Server PostInstallSetup Script
You must run the Process Server PostInstallSetup script.

1. Open a command prompt.
2. Navigate to the PostInstallSetup script in the following directory:
   On UNIX. <MDM Hub installation directory>/hub/cleanse
   On Windows. <MDM Hub installation directory>\hub\cleanse
3. Run the following command:
   On UNIX. postinstallsetup.sh -DwebspHERE.password=<webspHERE administrative user password>
   On Windows. postinstallsetup.bat -DwebspHERE.password=<webspHERE administrative user password>
4. Restart the application server.

Register the Operational Reference Stores
To register the Operational Reference Stores, use the Hub Console.

1. Start the Databases tool under the Configuration workbench.
2. Click Write Lock > Acquire Lock.
3. Click Register database.
   The Informatica MDM Hub Connection Wizard appears and prompts you to select the database type.
4. Select Microsoft SQL Server, Oracle, or IBM DB2, and click Next.
5. In Microsoft SQL Server, configure connection properties for the database.
   a. In the Connection Properties page, specify the connection properties, and then click Next.
The following table lists and describes the connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Display Name</td>
<td>Name for the Operational Reference Store that must appear in the Hub Console.</td>
</tr>
<tr>
<td>Machine Identifier</td>
<td>Prefix given to keys to uniquely identify records from the Hub Store instance.</td>
</tr>
<tr>
<td>Database hostname</td>
<td>IP address or name of the server that hosts the Microsoft SQL Server database.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the Microsoft SQL Server database. The default is 1433.</td>
</tr>
<tr>
<td>Schema Name</td>
<td>Name of the Operational Reference Store.</td>
</tr>
<tr>
<td>Password</td>
<td>Password associated with the user name for the Operational Reference Store.</td>
</tr>
<tr>
<td>Dynamic Data Masking host</td>
<td>IP address or name of the server that hosts Dynamic Data Masking. Leave empty if you do not use Dynamic Data Masking.</td>
</tr>
<tr>
<td>DDM connection URL</td>
<td>Optional. URL for the Dynamic Data Masking server. Leave empty if you do not use Dynamic Data Masking.</td>
</tr>
</tbody>
</table>

b. In the Connection Properties page, specify the connection properties, and then click Next.

c. Review the summary, and specify additional connection properties.

The following table lists additional connection properties that you can configure:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection URL</td>
<td>Connect URL. The Connection Wizard generates the connect URL by default.</td>
</tr>
<tr>
<td>Create datasource after registration</td>
<td>Select to create the datasource on the application server after registration.</td>
</tr>
</tbody>
</table>

6. In Oracle environments, configure connection properties for the database.

a. Select an Oracle connection method, and click Next.

The following table describes the Oracle connection methods that you can select:

<table>
<thead>
<tr>
<th>Connection Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Connect to Oracle by using the service name.</td>
</tr>
<tr>
<td>SID</td>
<td>Connect to Oracle by using the Oracle System ID.</td>
</tr>
</tbody>
</table>

For more information about SERVICE and SID names, see the Oracle documentation.

The Connection Properties page appears.

b. Specify the connection properties for the connection type that you select, and click Next.
The following table lists and describes the connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Display Name</td>
<td>Name for the Operational Reference Store that must appear in the Hub Console.</td>
</tr>
<tr>
<td>Machine Identifier</td>
<td>Prefix given to keys to uniquely identify records from the Hub Store instance.</td>
</tr>
<tr>
<td>Database hostname</td>
<td>IP address or name of the server that hosts the Oracle database.</td>
</tr>
<tr>
<td>SID</td>
<td>Oracle System Identifier that refers to the instance of the Oracle database running on the server. The SID field appears if you selected the SID connection type.</td>
</tr>
<tr>
<td>Service</td>
<td>Name of the Oracle SERVICE used to connect to the Oracle database. The Service field appears if you selected the Service connection type.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port of the Oracle listener running on the Oracle database server. The default is 1521.</td>
</tr>
<tr>
<td>Oracle TNS Name</td>
<td>Name by which the database is known on your network as defined in the TNSNAMES.ORA file of the application server. For example: mydatabase.mycompany.com. You set the Oracle TNS name when you install the Oracle database. For more information about the Oracle TNS name, see the Oracle documentation.</td>
</tr>
<tr>
<td>Schema Name</td>
<td>Name of the Operational Reference Store.</td>
</tr>
<tr>
<td>User name</td>
<td>User name for the Operational Reference Store. By default, this is the user name that you specify in the script that you use to create the Operational Reference Store. This user owns all of the Operational Reference Store database objects in the Hub Store. If a proxy user is configured for the Operational Reference Store, then you can specify the proxy user instead.</td>
</tr>
<tr>
<td>Password</td>
<td>Password associated with the user name for the Operational Reference Store. For Oracle, the password is not case sensitive.  By default, this is the password that you specify when you create the Operational Reference Store. If a proxy user is configured for the Operational Reference Store, then you specify the password for the proxy user instead.</td>
</tr>
<tr>
<td>Dynamic Data Masking host</td>
<td>IP address or name of the server that hosts Dynamic Data Masking. Leave empty if you do not use Dynamic Data Masking.</td>
</tr>
<tr>
<td>DDM connection URL</td>
<td>Optional. URL for the Dynamic Data Masking server. Leave empty if you do not use Dynamic Data Masking.</td>
</tr>
</tbody>
</table>

**Note:** The Schema Name and the User Name are both the names of the Operational Reference Store that you specified when you created the Operational Reference Store. If you need this information, consult your database administrator.

The Summary page appears.
c. Review the summary, and specify additional connection properties.

The following table lists additional connection properties that you can configure:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection URL</td>
<td>Connect URL. The Connection Wizard generates the connect URL by default. The following list shows the format of the connect URL for the Oracle connection types: Service connection type: jdbc:oracle:thin:@//database_host:port/service_name SID connection type: jdbc:oracle:thin:@//database_host:port:sid For a service connection type only, you have the option to customize and later test a different connection URL.</td>
</tr>
<tr>
<td>Create datasource after registration</td>
<td>Select to create the datasource on the application server after registration. Note: If you do not select the option, you must manually configure the data source.</td>
</tr>
</tbody>
</table>

For a service connection type, if you want to change the default URL, click the Edit button, specify the URL, and then click OK.

7. In IBM DB2 environments, configure connection properties for the database.
   a. Specify the connection properties, and click Next.

The following table lists and describes the connection properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Display Name</td>
<td>Name for the Operational Reference Store that must appear in the Hub Console.</td>
</tr>
<tr>
<td>Machine Identifier</td>
<td>Prefix given to keys to uniquely identify records from the Hub Store instance.</td>
</tr>
<tr>
<td>Database server name</td>
<td>IP address or name of the server that hosts the IBM DB2 database.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of the database that you create.</td>
</tr>
<tr>
<td>Database hostname</td>
<td>IP address or name of the server that hosts the IBM DB2 database.</td>
</tr>
<tr>
<td>Schema Name</td>
<td>Name of the Operational Reference Store.</td>
</tr>
<tr>
<td>User name</td>
<td>User name for the Operational Reference Store. By default, this is the user name that you specify in the script that you use to create the Operational Reference Store. This user owns all the Operational Reference Store database objects in the Hub Store. If a proxy user is configured for the Operational Reference Store, then you can specify the proxy user instead.</td>
</tr>
</tbody>
</table>
**Property** | **Description**
--- | ---
Password | Password associated with the user name for the Operational Reference Store. For IBM DB2, the password is case sensitive. By default, this is the password that you specify when you create the Operational Reference Store. If a proxy user is configured for the Operational Reference Store, then you specify the password for the proxy user instead.
Dynamic Data Masking host | IP address or name of the server that hosts Dynamic Data Masking. Leave empty if you do not use Dynamic Data Masking.
DDM connection URL | Optional. URL for the Dynamic Data Masking server. Leave empty if you do not use Dynamic Data Masking.

**Note:** The **Schema Name** and the **User Name** are both the names of the Operational Reference Store that you specified when you created the Operational Reference Store. If you need this information, consult your database administrator.

The **Summary** page appears.

b. Review the summary, and specify additional connection properties.

The following table lists additional connection properties that you can configure:

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection URL</td>
<td>Connect URL. The Connection Wizard generates the connect URL by default. The following example shows the format of the connect URL: jdbc:db2://database_host:port/db_name</td>
</tr>
<tr>
<td>Create datasource after registration</td>
<td>Select to create the datasource on the application server after registration. <strong>Note:</strong> If you do not select the option, you must manually configure the data source.</td>
</tr>
</tbody>
</table>

8. Click **Finish**.

The **Registering Database** dialog box appears.

9. Click **OK**.

The **Application Server Login** dialog box appears.

10. Enter the WebSphere administrative user name and password.

11. Click **OK**.

The MDM Hub registers the ORS.

12. Restart the application server.

13. Select the Operational Reference Store that you registered, and click the **Test database connection** button to test the database settings.

The Test Database dialog box displays the result of the database connection test.

14. Click **OK**

The ORS is registered, and the connection to the database is tested.
Configure Cleanse Functions for Platform Transformations

If you want to use the platform transformations that you configured, add an IDQ library in the Cleanse Functions tool. You can then use the cleanse functions in the library in place of the platform transformations.

1. Launch the Hub Console and start the **Cleanse Functions** tool.
2. Acquire a write lock.
3. Right-click **Cleanse Functions**, and then click **Add IDQ Library**.
   The **Add IDQ Library** dialog box appears.
4. Specify the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library Name</td>
<td>Name of the IDQ library. The name appears as the folder name in the Cleanse Functions list.</td>
</tr>
<tr>
<td>IDQ WSDL URI</td>
<td>URI of the WSDL associated with the platform transformation.</td>
</tr>
<tr>
<td>IDQ WSDL Service</td>
<td>Service of the WSDL associated with the platform transformation.</td>
</tr>
<tr>
<td>IDQ WSDL Port</td>
<td>Port of the WSDL associated with the platform transformation.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the library that you want displayed in the Cleanse Functions tool.</td>
</tr>
</tbody>
</table>

5. Click **OK**.
   The IDQ library appears in the Cleanse Functions navigator.
6. Click **Refresh** to generate the IDQ library.
   The Cleanse Functions tool retrieves the WSDL associated with the platform transformation, generates the IDQ library, and displays the available cleanse functions in the Cleanse Functions list.
7. Test the cleanse functions.
   You can now use the cleanse functions in place of the platform transformations. The cleanse functions in the IDQ library can call the web services associated with the platform transformations.

Validate the Upgraded Metadata

Ensure the Operational Reference Stores (ORS) do not have any validation errors. Compare the results with the previous validation results that you obtained in before the upgrade. Use the Repository Manager in the Hub Console to validate metadata.

**Note:** After you upgrade from a previous version of the MDM Hub, you might have validation errors for old databases that had staging tables without any mappings. In the Repository Manager tool in the Hub Console, click the **Repair** button to fix these repairable issues.
Validating Metadata

To validate the metadata of an Operational Reference Store (ORS) repository, use the Repository Manager tool in the Hub Console.

1. From the Configuration workbench in the Hub Console, select the Repository Manager tool.
2. From the Repository Manager tool, select the Validate tab.
3. From the Select the repository to validate list, select a repository.
4. Click the Validate button.
5. From the Select Validation Checks dialog box, select the validation checks to perform. Click OK.
   The Repository Manager tool validates the repository and displays any issues in the Issues Found pane.
6. Click the Repair button to fix repairable issues.
7. If the ORS remains in the Unknown state, synchronize the system clocks of the application server and the database machine.

Saving the Validation Results

After you run the validation process, you can save the validation results as an HTML file.

1. From the Repository Manager tool in the Hub Console, select the Validate tab.
2. Click the Save button.
3. From the Save dialog box, navigate to the directory where you want to save the validation results.
4. Specify a descriptive file name for the HTML file. Click Save.
   The Repository Manager saves the validation results as an HTML file in the specified location.

Resolving Metadata Validation Messages

After you run the validation tool, you might receive validation messages.

The following error messages are some of the most common validation messages.

Warning SIP-PV-10703 Package 'EMPLOYEEDETAILS_PKG' is not synchronized with its database view.

To synchronize with the database view, run the Repair process from the Repository Manager.

View 'C_EMPLOYEEDETAILS_MTIP' - SELECT privilege for proxy user role is not granted. or SIP-MV-11410 - SQL of the root MTIP is incorrect.

Rebuild the MTIP views.

1. In the Hub Console, open the Configuration workbench and click Enterprise Manager.
2. Acquire a write lock.
3. Select the ORS databases tab.
4. Select the database.
5. Select the Properties tab.
6. Find the property called MTIP regeneration required, and click the Regenerate MTIPs button.
Review the MDM Hub Environment Report

Use the Enterprise Manager tool in the Hub Console to review the current MDM Hub configuration for Hub Servers, Process Servers, the MDM Hub Master Database, and Operational Reference Store databases. Note the version history of the components.

Save a copy of the environment report in the upgradedoc upgrade documentation folder.

Saving the MDM Hub Environment Report

To save the MDM Hub environment report, use the Enterprise Manager tool in the Hub Console.

1. From the Configuration workbench in the Hub Console, select the Enterprise Manager tool.
2. From the Enterprise Manager tool, select the Environment Report tab.
3. Click Save.
4. From the Save Hub Environment Report dialog box, navigate to the directory where you want to save the environment report.
5. Click Save.
Upgrading the SiperianClient Library Classes for the EJB Protocol

If you use the EJB protocol to communicate with the MDM Hub through the Services Integration Framework (SIF) requests, you must use the latest version of the SiperianClient library classes. If you use custom JNDI lookup methods, update the lookup methods so that the methods conform to the EJB3 conventions.

1. Replace the existing SiperianClient library classes with the latest version of the SiperianClient library classes.
   
   The `siperian-api.jar` file located in the following directories contains the SiperianClient library classes:
   - `<Resource Kit Installation Directory>\sdk\sifsdk\lib`
   - `<MDM Hub Installation Directory>\hub\server\lib`

2. If you use custom JNDI lookup methods, update the lookup methods so that the methods conform to the EJB3 conventions.

Prepare the MDM Hub Metadata

<table>
<thead>
<tr>
<th>Upgrade Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regenerate match tokens.</td>
<td>Run the Generate Match Tokens batch job for each base object. The Generate Match Tokens batch job creates the match tokens based on the SSA-Name3 library files that you update during the Process Server upgrade.</td>
</tr>
<tr>
<td>Reindex the search data.</td>
<td>If the search data contains any accented characters, such as à and í, you can run the Initially Index Smart Search Data batch job to reindex the data. After you reindex the data, a search request can return records that contain accented characters.</td>
</tr>
<tr>
<td>Configure metadata caching (Optional)</td>
<td>In version 10.1 and earlier, the MDM Hub used JBoss Cache for metadata caching. After you upgrade from one of these versions, the MDM Hub Server uses the Infinispan configuration file instead of the JBoss Cache configuration file. You might need to configure Infinispan caching to achieve similar results as JBoss Cache. For more information, see &quot;Configuring Metadata Caching (Optional)&quot; on page 162.</td>
</tr>
<tr>
<td>Reregister custom indexes.</td>
<td>You must reregister custom indexes after the migration. Use the registerCustomIndex SIF API to reregister the custom indexes. For more information about the RegisterCustomIndex SIF API, see the Multidomain MDM Services Integration Framework Guide. For SOAP and Java code samples to run the registerCustomIndex SIF API, see KB 500116. <a href="https://kb.infor.com/howto/6/Pages/19/500116.aspx?myk=500116">https://kb.infor.com/howto/6/Pages/19/500116.aspx?myk=500116</a>.</td>
</tr>
</tbody>
</table>

Upgrade Tests

Test the upgraded MDM Hub. Each Multidomain MDM implementation is unique and the testing requirements vary between the development, test, and production environments. If a suggested upgrade test is not
appropriate for your environment, you can design your own tests. Design the test activities to meet the unique requirements of your implementation.

**MDM Hub Upgrade Tests**

Perform the following Hub Console upgrade tests that apply to your environment:

1. Launch the Hub Console.
2. Select the **Users** tool in the **Configuration** workbench to view the properties of an existing user.
3. Select the **Schema Viewer** tool in the **Model** workbench, and then connect to an Operational Reference Store. Review the schema in the **Schema Viewer**.
4. Select the **Schema** tool in the **Model** workbench to view the **Match/Merge Setup** for a base object.
5. Select the **Batch Viewer** tool in the **Utilities** workbench. If possible, run test batch jobs for the Stage batch job, the Load batch job, the Match batch job, and the Merge batch job.
7. Select the **Cleanse Functions** tool in the **Model** workbench. Run a test cleanse function for each external cleanse engine.
8. Select the **Data Manager** tool in the **Data Steward** workbench. Create two matching test records.
9. Select the **Merge Manager** tool in the **Data Steward** workbench. Find the two test records, merge the test records, and then unmerge the test records.

**Custom Code Upgrade Tests**

If you have custom code such as custom client applications, run tests to verify that the custom code works as expected.

**Provisioning Tool Upgrade Test**

Log in to the Provisioning tool. The tool validates the XML files that contain your configuration for business entities, reference entities, applications, custom views, tasks, and so on.

If the validation process is successful, continue to the next upgrade test. Optionally, you can spot check your configuration to verify the settings.

If the validation process detects some errors, review the list of errors and proposed fixes. A fix might include removing some settings. You can choose to accept all the fixes or cancel without making changes. If you choose to cancel, you must fix the errors in the XML files yourself. The XML files are stored in the C_REPOS_CO_CS_CONFIG and C_REPOS_COMPONENT_INSTANCE repository tables.

**Caution:** If you exit without fixing the errors, you might be locked out of the Provisioning tool.

1. Log in to the Provisioning tool.
2. Select an Operational Reference Store database.
3. If you see validation errors, review the proposed fixes.
   - To apply the fixes, click **Fix**.
   - To exit without applying the fixes, click **Cancel**.
     You are logged out of the Provisioning tool. Open the XML files and fix the errors.
4. Optionally, after the XML is valid, you can verify the configuration settings.
Data Director with Business Entities Upgrade Tests

If you use Data Director with business entities, open the application and test it.

Perform the following upgrade tests that apply to your environment:

1. Log in to Data Director.
2. Run multiple searches.
3. Create and process multiple tasks.
4. Insert a test record.
5. Copy the test record to create a second test record.
6. Run a search to find the two test records.
7. Merge and unmerge the two test records.

Data Director with Subject Areas Upgrade Tests

If you use Data Director with subject areas, you need to deploy the application before you begin the tests.

Perform the following upgrade tests that apply to your environment:

1. Launch the Data Director Configuration Manager, and then deploy a Data Director application instance.
2. Log in to Data Director.
3. Run multiple searches.
4. Create and process multiple tasks.
5. Insert a test record.
6. Copy the test record to create a second test record.
7. Run a search to find the two test records.
8. Merge and unmerge the two test records.

Data Director and Hub Server Properties

The upgrade process preserves the values of the Hub Server properties that affect Data Director.

When you upgrade from earlier versions, the pre-upgrade `cmxserver.properties` file does not contain some properties that were added in version 10.0.0 and later. Verify that the upgrade process added the properties to the `cmxserver.properties` file. If necessary, add any missing properties to the end of the `<MDM Hub installation directory>/hub/server/resources/cmxserver.properties` file.

The default values for the properties retain the current behavior of Data Director applications. Before you customize the properties, read the property descriptions in the "Hub Server Properties" chapter of the Multidomain MDM Configuration Guide.

Properties Added in Version 10.3

Added new properties to support file upload, task manager, and workflow diagrams.

```bash
# File upload properties
# ------------------------
# Maximum upload size.
cmx.file.max_file_size_mb=20
```
# Maximum number of concurrent uploads.
cmx.file.max_concurrent_uploads=20
# Type of files that can be uploaded.
cmx.file.allowed_file_extensions=pdf,jpg
# Number of minutes until an uploaded file expires.
cmx.server.attachment.temp.ttl_minutes=60

# Task Manager property
# -----------------------------
# Set to true to display the Task Manager tab in applications
# that use subject areas.
cmx.dataview.taskmanager.enabled=true

# Workflow diagram properties
# -----------------------------
# Set to true to display the workflow diagram associated
# with the tasks in the Task Manager for the users with
# the ActiveVOS abAdmin role.
cmx.e360.BPMProcess.view.enabled=false
cmx.e360.BPMProcess.view.autologout.seconds=30

Note: If you decide to use Elasticsearch for full-text search in a Data Director application, add the
Elasticsearch properties manually. For more information, see "Search Configuration Upgrade Overview" on
page 123.

Properties Added in Version 10.2 and earlier

Added properties to support the Data tab, search, and the Entity 360 framework. Add the default values and
then change them as needed.

# View properties
# ---------------
# Show or hide the views for subject areas.
cmx.dataview.enabled=true
# Show or hide the views for business entities.
cmx.e360.view.enabled=false
# Show or hide the Cross-reference view and Match view.
cmx.e360.match_xref.view.enabled=false

# Search with Solr (formerly Smart Search) properties
# -----------------------------------------------
# Set to true to use Solr for search.
cmx.ss.enabled=false

Data Director Global Properties

If your Data Director environment included user preferences for shown or hidden columns, the settings are
lost when you upgrade because the cryptographic hash algorithm has changed in this version. After you
upgrade, clear the C_REPOS_DS_PREF_DETAIL table and recreate your user preferences.

For instructions about how to update Data Director global properties, including user preferences, see the
Multidomain MDM Data Director Implementation Guide.
Generate the Business Entity Schema

If you use business entity services, you must generate the business entity schema after you upgrade. You can generate the business entity schema, use the Informatica Data Director Configuration Manager.

Back up and customized business entity or business entity service configuration files before you generate the business entity schema.

To generate the business entity schema from the Informatica Data Director Configuration Manager, in the Applications screen, click Generate Business Entity Schema.
Search Configuration Upgrade Overview

You can use a Data Director application or a custom application to search for data within a specific business entity. Previously, you used configured Solr for search operations, which is now deprecated. Informatica recommends that you configure Elasticsearch for search operations, which is packaged with the MDM Hub installer.

The performance of searches with Elasticsearch is better than the searches with Solr. Also, to use security filters during search, you must configure Elasticsearch for search.

To upgrade the search configuration to use Elasticsearch, perform the following tasks:

1. Set up Elasticsearch.
2. Configure the MDM Hub properties for search.
3. Configure search by using the Provisioning tool.
4. Validate the Operational Reference Store (ORS).
5. Index the search data.

Step 1. Set Up Elasticsearch

To configure search, you must set up Elasticsearch.

1. Install Elasticsearch.
2. Create keystores, truststore, and certificates.
3. Configure the Elasticsearch Java Virtual Machine (JVM).
5. Secure the Elasticsearch cluster.
6. Upload the Search Guard configuration to Elasticsearch.
7. Configure the client certificate DN in the Elasticsearch properties file
8. Customize the list of words to ignore in searches.
9. Customize the list of synonyms to include in searches.
10. Start Elasticsearch.

**Install Elasticsearch**

After you install the Hub Server and the Process Server, to configure search, install Elasticsearch. To install Elasticsearch, you extract the Elasticsearch archive file.

Ensure that you use a supported operating system and Java version for your Elasticsearch installation. For more information, see the Elasticsearch Support Matrix.

1. Navigate to the Elasticsearch ZIP file in the following directory:
   `<MDM_hub_installation_directory>/hub/server/thirdparty`
2. Extract `elasticsearch-<version>.zip`.

**Create Keystores, Truststore, and Certificates**

After you install Elasticsearch, create keystores, truststore, and security certificates that are required to secure the communication between the MDM Hub and Elasticsearch. To create keystores, truststore, and certificates, run the `sip_ant` script on only one of the machines that has the Hub Server installed. Then, copy the keystores, truststore, and certificates to all the other machines on which the Hub Server is installed.

**Note:** You can create keystores, truststore, and certificates without using the `sip_ant` script.

The following table describes the keystores and truststore that are required:

<table>
<thead>
<tr>
<th>Keystore/Truststore Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDM_ESCLIENT_FILE_JKS.keystore</td>
<td>Elasticsearch keystore that contains the client certificate and its key.</td>
</tr>
<tr>
<td>MDM_ESKEYSTORE_FILE_JKS.keystore</td>
<td>Elasticsearch keystore that contains the client and node certificates. If the Elasticsearch cluster has multiple nodes, all the nodes use the certificates.</td>
</tr>
<tr>
<td>MDM_ESTRUSTSTORE_FILE_JKS.keystore</td>
<td>Elasticsearch truststore that contains the signed certificate for the client and Elasticsearch nodes.</td>
</tr>
</tbody>
</table>

1. Open a command prompt, and navigate to the following directory on one of the machines that has the Hub Server installed:
   `<MDM_hub_installation_directory>/hub/server/bin`
2. To create the keystores, truststore, and certificates, run the following command:
   - On UNIX, `./sip_ant.sh generate_mdm_es_store`
   - On Windows, `sip_ant.bat generate_mdm_es_store`
3. When prompted for a password for the keystores and truststore, specify a password.
The keystores, truststore, and certificates are created in the following directory:
<MDM Hub installation directory>/hub/server/resources/certificates

4. Copy the following keystores and truststore to the <Elasticsearch installation directory>/config directory of each Elasticsearch installation:
   - MDM_ESCLIENT_FILE_JKS.keystore
   - MDM_ESKEYSTORE_FILE_JKS.keystore
   - MDM_ESTRUSTSTORE_FILE_JKS.keystore

5. Copy the following keystore and truststore to the <MDM Hub installation directory>/hub/server/resources/certificates directory of each Hub Server node that is part of the Elasticsearch cluster:
   - MDM_ESCLIENT_FILE_JKS.keystore
   - MDM_ESTRUSTSTORE_FILE_JKS.keystore

Configure the Elasticsearch Java Virtual Machine (JVM)

Configure the Elasticsearch Java Virtual Machine (JVM) to use a heap size based on the amount of RAM available on your machine. To configure the JVM, edit the jvm.options file.

1. Find the jvm.options file in the following directory:
   <Elasticsearch installation directory>/config

2. Use a text editor to open the file, and edit the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Xms</td>
<td>Minimum heap size. Default is 1 GB.</td>
</tr>
<tr>
<td>-Xmx</td>
<td>Maximum heap size. Default is 1 GB.</td>
</tr>
<tr>
<td>-XX:HeapDumpPath</td>
<td>Heap dump path. Default is /var/lib/elasticsearch. In a multi-cluster environment, you must set this property to an alternative path.</td>
</tr>
</tbody>
</table>

Note: Set the minimum heap size (Xms) and the maximum heap size (Xmx) to the same value. Use the default settings for other properties.

Configure the Elasticsearch Properties File

Informatica provides a sample Elasticsearch properties file. To configure Elasticsearch, edit the properties file.

1. Find the elasticsearch.yml file in the following directory:
   <Elasticsearch installation directory>/config
2. Use a text editor to open the file, and edit the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bootstrap.memory_lock</code></td>
<td>Sets up memory locking. To prevent any Elasticsearch memory from being swapped out, set to <code>true</code>. Default is <code>true</code>.</td>
</tr>
<tr>
<td><code>cluster.name</code></td>
<td>Specify a unique name for the Elasticsearch cluster. If you have multiple clusters, ensure that the name of each cluster is unique. If a cluster has multiple nodes, ensure that on each node of the cluster, the same cluster name is specified.</td>
</tr>
<tr>
<td><code>discovery.zen.minimum_master_nodes</code></td>
<td>Required for a multi-node cluster to prevent data loss and maintain cluster stability. Set to the following value: <code>(number of master-eligible nodes / 2) + 1</code> For example, if a cluster has three nodes, all of which are master-eligible nodes and can contain data, then set the property to <code>(3 / 2) + 1</code>, which is rounded to 2.</td>
</tr>
<tr>
<td><code>discovery.zen.ping.unicast.hosts</code></td>
<td>Required for a multi-node cluster. This property is used to specify the discovery setting, which is a list of IP addresses and transport ports of the nodes in the cluster. Use the following format to set the property: <code>[&quot;host1:port1&quot;,&quot;host2:port2&quot;,&quot;host3:port3&quot;]</code></td>
</tr>
<tr>
<td><code>http.port</code></td>
<td>Port for the HTTP requests. Default is 9200.</td>
</tr>
<tr>
<td><code>network.host</code></td>
<td>The IP address of the host to use as the bind address.</td>
</tr>
<tr>
<td><code>node.data</code></td>
<td>Enables a node as a data node that performs data related operations, such as CRUD and search. Default is <code>true</code>.</td>
</tr>
<tr>
<td><code>node.ingest</code></td>
<td>Enables a node as an ingest node that transforms and enriches the data before indexing. Default is <code>true</code>.</td>
</tr>
<tr>
<td><code>node.master</code></td>
<td>Enables a node as a master node that controls the cluster. If a cluster has multiple nodes, enable at least one of the nodes as a master node. For high availability, set multiple nodes as master nodes. Default is <code>true</code>.</td>
</tr>
<tr>
<td><code>node.name</code></td>
<td>Specify a unique name for the node.</td>
</tr>
<tr>
<td><code>path.data</code></td>
<td>Path to the directory where you want to store the data. You can configure multiple data directories. For more information about configuring multiple data directories, see the Elasticsearch documentation.</td>
</tr>
<tr>
<td><code>path.logs</code></td>
<td>Path to the log files.</td>
</tr>
<tr>
<td><code>transport.tcp.port</code></td>
<td>The TCP bind port. Default is 9300.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>searchguard.enterprise_modules_enabled</td>
<td>Specifies whether you want to enable Search Guard Enterprise Edition. To avoid license violation, always set the property to false. The MDM Hub installer includes Search Guard Community Edition, which is free. Informatica does not include a license for Search Guard Enterprise Edition.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.keystore_type</td>
<td>The type of keystore file. Set to JKS. Default is JKS.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.keystore_filepath</td>
<td>Relative path to the keystore file. If you used the sip_ant script to create the keystore, use the default path. Default is MDM_ESKEYSTORE_FILE_JKS.keystore.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.keystore_password</td>
<td>The keystore password. Default is info@1234.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.truststore_type</td>
<td>The type of truststore file. Set to JKS. Default is JKS.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.truststore_filepath</td>
<td>Relative path to the truststore file. If you used the sip_ant script to create the truststore, use the default path. Default is MDM_ESTRUSTSTORE_FILE_JKS.keystore.</td>
</tr>
<tr>
<td>searchguard.ssl.transport.truststore_password</td>
<td>The truststore password. Default is info@1234.</td>
</tr>
<tr>
<td>searchguard.ssl.http.enabled</td>
<td>Specifies whether you want to enable transport layer security (TLS) on the REST layer. Set to true. Default is true.</td>
</tr>
<tr>
<td>searchguard.ssl.http.clientauth_mode</td>
<td>Specifies whether you want to use the TLS client authentication mode on the REST layer. Set to REQUIRE. Default is REQUIRE.</td>
</tr>
<tr>
<td>searchguard.ssl.http.keystore_type</td>
<td>The type of keystore file. Set to JKS. Default is JKS.</td>
</tr>
<tr>
<td>searchguard.ssl.http.keystore_filepath</td>
<td>Relative path to the keystore file. If you used the sip_ant script to create the keystore, use the default path. Default is MDM_ESCLIENT_FILE_JKS.keystore.</td>
</tr>
<tr>
<td>searchguard.ssl.http.keystore_password</td>
<td>The keystore password. Default is info@1234.</td>
</tr>
<tr>
<td>searchguard.ssl.http.truststore_type</td>
<td>The type of truststore file. Set to JKS. Default is JKS.</td>
</tr>
<tr>
<td>searchguard.ssl.http.truststore_filepath</td>
<td>Relative path to the truststore file. If you used the sip_ant script to create the truststore, use the default path. Default is MDM_ESTRUSTSTORE_FILE_JKS.keystore.</td>
</tr>
<tr>
<td>searchguard.ssl.http.truststore_password</td>
<td>The truststore password. Default is info@1234.</td>
</tr>
</tbody>
</table>
### Secure the Elasticsearch Cluster

To secure the Elasticsearch cluster, configure the Search Guard security plugin. To configure the security plugin, edit the Search Guard sample configuration files, which include the required settings.

**Note:** If you use certificates created by the `sip_ant` script, do not edit the sample configuration files.

1. Find the Search Guard sample configuration files in the following directory:
   `<elasticsearch installation directory>/plugins/search-guard=6/sgconfig`
2. If you did not use the `sip_ant` script to create the security certificates, use a text editor to open the files, and edit the parameters.

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>Purpose</th>
<th>Required Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sg_config.yml</code></td>
<td>Authentication and authorization configuration</td>
<td>Update the <code>username_attribute</code>. Default is <code>cn</code>.</td>
</tr>
<tr>
<td><code>sg_roles.yml</code></td>
<td>User role configuration</td>
<td>Add the <code>sg_mdm_access</code> role for the MDM Hub. The role is required, because the client and administrator certificates for Elasticsearch are different and need to be mapped to this role.</td>
</tr>
<tr>
<td><code>sg_role_mapping.yml</code></td>
<td>User role mappings configuration</td>
<td>Map the common name of the client certificate to the <code>sg_mdm_access</code> role. By default, the administrator and client roles are mapped to the common name of the client certificate <code>CN=EsClient</code>.</td>
</tr>
</tbody>
</table>

For more information about Search Guard configuration files, see the Search Guard documentation.
Upload the Search Guard Configuration to Elasticsearch

To upload the Search Guard configuration to Elasticsearch, use the Search Guard sgadmin tool. You can upload the configuration from any machine that has access to your Elasticsearch cluster. When you upload the configuration, Search Guard is initialized and Elasticsearch is secured.

1. Open a command prompt, and run the following command:
   
   ```bash
   sgadmin.bat -h <IP address of the host> -p <bind port>
   -cd <elasticsearch installation directory>/plugins/search-guard-6/sgconfig
   -ks <elasticsearch installation directory>/config/MDM_ESCLIENT_FILE_JKS.keystore
   -kspass <password>
   -ts <elasticsearch installation directory>/config/MDM_ESTRUSTSTORE_FILE_JKS.keystore
   -tspass <password>
   -cn <cluster name>
   -nhrv -tst JKS -kst JKS
   ```

   **Note:** If the cluster has a single node, remove `-cn <cluster name>` from the command.

   After you upload the Search Guard configuration, ensure that you start each node of the Elasticsearch cluster for the changes to take effect.

Configure the Client Certificate DN in the Elasticsearch Properties File

After you initialize and secure Elasticsearch by uploading the Search Guard configuration to Elasticsearch, configure the DN of a client certificate.

**Note:** Ensure that the client certificate for which you configure the DN is not an administrative certificate.

1. Find the `elasticsearch.yml` file in the following directory:
   
   `<elasticsearch installation directory>/config`

2. Use a text editor to open the file, and edit the `searchguard.authcz.admin_dn` property.
   
   The default is `- CN=EsClient`. Change the default value. Set the DN of a client certificate that is not an administrative certificate.

3. Save and close the file.

Customize the List of Words to Ignore in Searches

When you perform a search, the MDM Hub ignores common words such as "and", "an", and "is". You can use the default list of common words to ignore in a search or you can customize the list. To customize the list of words to ignore in a search, edit the `stopwords.txt` file.

1. Use a text editor to open the `stopwords.txt` file in the following location:
   
   `<elasticsearch installation directory>/config/analysis`

2. Edit and save the `stopwords.txt` file.

3. If data was indexed before you edited the `stopwords.txt` file, manually delete the indexes, restart Elasticsearch, and then, reindex the data.

For more information about updating the `stopwords.txt` file, see the Elasticsearch documentation.
Customize the List of Synonyms to Include in Searches

When you perform a search, the MDM Hub can search for synonyms of the search string that you specify. For example, when you search for "William", the search result includes the synonyms "Will" and "Willy". You can define the synonyms in the `synonyms.txt` file.

To customize the synonyms to use in a search, edit the `synonyms.txt` file.

1. Use a text editor to open the `synonyms.txt` file in the following location:
   `<elasticsearch installation directory>/config/analysis`

2. Edit and save the `synonyms.txt` file.

3. If data was indexed before you edited the `synonyms.txt` file, manually delete the indexes, restart Elasticsearch, and then, reindex the data.

For more information about updating the `synonyms.txt` file, see the Elasticsearch documentation.

Start Elasticsearch

After you set up Elasticsearch, start each node of the Elasticsearch cluster for the changes to take effect.

1. Open a command prompt, and change to the following directory:
   `<elasticsearch installation directory>/bin`

2. Run the following command:
   - On UNIX, `elasticsearch.sh`
   - On Windows, `elasticsearch.bat`

Step 2. Configure the MDM Hub Properties for Search

To configure the MDM Hub properties, use the Hub Console, the Process Server properties file, and the Hub Server properties file.

1. Configure the Process Server properties.

2. Configure the Hub Server properties.

Configure the Hub Server for Search

You must configure all the Hub Server instances to enable search. Use the Hub Server tool in the Hub Console and the `cmxserver.properties` file to configure the Hub Server properties for search.

1. Use a text editor to open the `cmxserver.properties` file in the following location: `<MDM Hub Installation Directory>\hub\server\resources\cmxserver.properties`
2. Configure the following properties for search:

- **cmx.ss.engine**
  Required if you want to use the Elasticsearch engine for search. Manually add the property and set to `es`.

- **cmx.ss.dirtyIndex.disable**
  Applicable to the Solr search engine and will be deprecated. Set to `true` for Elasticsearch. Default is `false`.

- **ex.max.conn.per.host**
  Sets the maximum number of Elasticsearch nodes that you want to connect to the host. Set to the number of Elasticsearch cluster nodes on the host.

- **ex.max.threads**
  Sets the maximum number of threads that you want the Apache asynchronous non-blocking receiver to use for each node in the Elasticsearch cluster. Default is 1. Change the value only when suggested by Informatica Global Customer Support.

- **es.index.refresh.interval**
  Sets the interval, in seconds, for Elasticsearch to commit the changes to the data after an Initially Index Smart Search Data batch job is run. The data is available for search after this time interval. Default is 30.
  This property impacts the high indexing volume encountered during initial indexing. Change the value only when suggested by Informatica Global Customer Support.

- **ssl.keyStore**
  Required if you use the HTTPS port of the application server to configure the Hub Server. Manually add the property. Absolute path and file name of the keystore file.

- **ssl.keyStore.password**
  Required if you use the HTTPS port of the application server to configure the Hub Server. Manually add the property. Plain text password for the keystore file.

- **ssl.trustStore**
  Required if you use the HTTPS port of the application server to configure the Hub Server. Manually add the property. Absolute path and file name of the truststore file.

- **ssl.trustStore.password**
  Required if you use the HTTPS port of the application server to configure the Hub Server. Manually add the property. Plain text password for the truststore file.

After you update the Hub Server properties, you must validate the Operational Reference Store (ORS), and restart the Hub Console.

### Configure Process Servers for Search

When you configure search with Elasticsearch, enable search on all the Process Server instances. Use the Process Server tool in the Hub Console and the `cmxcleanse.properties` file to configure the Process Server properties for search.

1. In the Hub Console of a node, start the Process Server tool.
2. Click **Write Lock > Acquire Lock**.
3. In the right pane of the Process Server tool, click the **Add Process Server** button.
The **Add/Edit Process Server** dialog box appears.

4. Set the following properties of a Process Server for search:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Search Processing</td>
<td>Indicates whether to enable search on the Process Server. Ensure that you select the option to enable search.</td>
</tr>
<tr>
<td>Enable ZooKeeper</td>
<td>Indicates whether to use the Process Server as the ZooKeeper server for the search configuration with Solr. For search with Elasticsearch, ensure that you clear the option to disable ZooKeeper.</td>
</tr>
</tbody>
</table>

5. Click **OK**, and then click **Save**.

6. Edit the **cmxcleanse.properties file**.

   The **cmxcleanse.properties file in the following location:** `<MDM Hub Installation Directory>/hub\cleanserlurc\resources`

   a. Configure the following properties for search:

      **cmx.ss.engine**

      Required if you want to use the Elasticsearch engine for search. Manually add the property and set to `es`.

      **ex.max.conn.per.host**

      Sets the maximum number of Elasticsearch nodes that you want to connect to the host. Set to the number of Elasticsearch cluster nodes on the host.

      **ex.max.threads**

      Sets the maximum number of threads that you want the Apache asynchronous non-blocking receiver to use for each node in the Elasticsearch cluster. Default is 1. Change the value only when suggested by Informatica Global Customer Support.

   b. Remove the following properties that are configured for search with Solr:

      - `solr.allowAdminConsole`
      - `zookeeper.tickTime`
      - `pingSolrOnStartup`

7. Save the **cmxcleanse.properties file**.

8. Restart the application server.

---

**Step 3. Configure Search by Using the Provisioning Tool**

After you set up Elasticsearch and configure the MDM Hub properties, use the Provisioning tool to configure the search environment.

1. Configure the Elasticsearch cluster.
2. Configure the search result views.
Configure the Elasticsearch Cluster

Use the Provisioning tool to configure the Elasticsearch cluster. The search APIs use the configuration. The Data Director application and any custom applications use the search APIs.

Note: When you configure the Elasticsearch cluster, only master nodes must be specified.

1. Open a supported browser, and enter the following URL:
   https://<MDM Hub Server host name>:<MDM Hub Server port number>/provisioning/
   The Login page appears.
2. Enter the user name and password, and click Log In.
3. Select the Operational Reference Store (ORS) for which you want to create the Elasticsearch cluster.
4. Click Configuration > Infrastructure Settings.
   The Infrastructure Settings page appears.
5. Select Elastic Search Cluster from the list, and click Create.
6. In the tree view, under ECluster, select esNode, and click Create.
7. Configure the following Elasticsearch cluster properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the master node in the Elasticsearch cluster.</td>
</tr>
<tr>
<td>URL</td>
<td>URL of the master node in the Elasticsearch cluster. The URL format is https://&lt;host name&gt;:&lt;port&gt;.</td>
</tr>
</tbody>
</table>

8. Click Apply.
9. If you want to create additional master nodes, repeat steps 6 through 8.
10. Publish the changes to the MDM Hub.
    a. Click Publish.
       A change confirmation dialog box appears that prompts you to confirm the changes.
    b. Review the changes, and click Confirm.
       A validation process runs on the application. A confirmation dialog box appears that prompts you to publish the changes.
    c. Click one of the following buttons:
       * Publish. Saves the changes to the MDM Hub.
       * No. The changes remain in the temporary workspace.

Configure the Search Result Views

You can use the Provisioning tool to configure the business entity views that you want to use for search. A search result includes only the fields that are part of the business entity view that you configure for search results.

Before you configure the searchable views, create the business entity views that you want to use for the search results.

1. Open a supported browser, and use the following URL to log into the Provisioning tool:
   https://<MDM Hub Server host name>:<MDM Server port number>/provisioning/
2. From the Database list, select the database with which your application is associated.

3. Click Configuration > Application Editor.
   
   The Applications page appears.

4. From the Applications list, select the application for which you want to configure search.
   
   If you do not have an application, create one before you can configure search.

5. In the tree view panel, click the Search Configuration node.

6. In the properties panel, for each business entity, select the search view.
   
   If you do not select a search view, the search results contain the full business entity.

7. Click Apply.
   
   The search views configuration is saved to the temporary workspace.

8. Publish the changes to the MDM Hub.
   
   a. Click Publish.
      
      A change confirmation dialog box appears that prompts you to confirm the changes.
   
   b. Review the changes, and click Confirm.
      
      A validation process runs on the application. A confirmation dialog box appears that prompts you to publish the changes.
   
   c. Click one of the following buttons:
      
      • Publish. Saves the changes to the MDM Hub.
      
      • No. The changes remain in the temporary workspace.

---

**Step 4. Validate the Operational Reference Store**

To validate the metadata of the Operational Reference Store (ORS) that is affected by the Elasticsearch configuration, use the Repository Manager tool in the Hub Console.

1. Start the Hub Console and connect to the MDM Hub Master Database.

2. Expand the Configuration workbench, and click Repository Manager.

   The Repository Manager appears.

3. Click the Validate tab, and select the repository to validate.

4. Click Validate.

   The Select Validation Checks dialog box appears.

5. Select the validation checks to perform.

6. Click OK.

   The Repository Manager validates the repository and displays any issues in the Issues Found pane.

7. To repair issues, click Repair.
Step 5. Index the Search Data

If your environment contains data, manually run the Initially Index Smart Search Data batch job to index the data. If your environment does not contain any data, you do not need to run the Initially Index Smart Search Data job. When you run the Load batch job to load data, the Load batch job automatically runs the Initially Index Smart Search Data batch job and indexes the data. A search request uses the indexes to search for records.

Run the Initially Index Smart Search Data batch job on all the base objects that contribute to the business entities. When you run the Initially Index Smart Search Data batch job on a base object, the Elasticsearch server indexes the data in the searchable fields. The job then adds the indexed data to all the collections that represent the business entities to which the searchable fields belong. If a collection is too large, you can split the collection into one or more shards. Shards are the logical pieces of a collection split over multiple nodes. When you perform a search, the Elasticsearch server reads the collections and returns the matching fields.

The Initially Index Smart Search Data batch job indexes the records asynchronously and reports successful completion after the job queues the indexing request for all the records. A search request can show the indexed records only after the successful completion of the index request, which might take a few minutes.

**Important**: If you update the searchable properties of a field after you index your data, the indexes are deleted. You must run the Initially Index Smart Search Data batch job to index the data. In addition, the indexing process is a resource-intensive process, so do not run multiple Initially Index Smart Search Data batch jobs in parallel.
ActiveVOS Post-Installation Tasks for the Application Server

Whether you perform a clean upgrade or an in-place upgrade, perform the ActiveVOS post-installation tasks for the application server to ensure your environment is properly configured.

For ActiveVOS post-installation tasks for the application server, see the ActiveVOS Post-Installation Tasks for the Application Server chapter in the Multidomain MDM Installation Guide that applies to your environment.
CHAPTER 12

ActiveVOS Post-Upgrade Tasks for Business Entity Adapter

This chapter includes the following topics:

- ActiveVOS Post-Upgrade Tasks for the Business Entity Adapter, 137
- Configuring the ActiveVOS URNs for the Business Entity Workflow Adapter, 138
- Set the ActiveVOS Protocol to HTTPS, 138
- Update Customized Workflows for Business Entities, 139
- Configure the MDM Identity Services for ActiveVOS, 142
- Custom BeMDMWorkflow Project (In-place Upgrade), 142
- Configure Unmerge and Merge Workflow Triggers (In-place Upgrade), 143
- Add the Entity 360 Framework Task Manager, 143

ActiveVOS Post-Upgrade Tasks for the Business Entity Adapter

Whether you perform a clean upgrade or an in-place upgrade, if you use the ActiveVOS workflow adapter based on business entities, perform the ActiveVOS post-upgrade tasks for the business entity adapter to ensure your environment is properly configured.
Configuring the ActiveVOS URNs for the Business Entity Workflow Adapter

The ActiveVOS Server has two predefined uniform resource names (URNs) that it uses internally. You need to update the URL in the URN mappings to use the host name and the port number where the ActiveVOS Server runs.

1. Launch the ActiveVOS Console. In a browser, type the following URL, substituting the correct host name and port number:
   - Encrypted connections: https://[host]:[port]/activevos
   - Non-encrypted connections: http://[host]:[port]/activevos

2. In the ActiveVOS Console, on the Home page, click Administration > Configure Server > URN Mappings.

3. For the following URNs, update the paths to reflect the host name and port number of the ActiveVOS Server:

<table>
<thead>
<tr>
<th>URN</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae:internal-reporting</td>
<td>Encrypted connections: https://[host]:[port]/activevos/internalreports</td>
</tr>
<tr>
<td></td>
<td>Non-encrypted connections: http://[host]:[port]/activevos/internalreports</td>
</tr>
<tr>
<td>ae:task-inbox</td>
<td>Encrypted connections: https://[host]:[port]/activevos-central/avc</td>
</tr>
<tr>
<td></td>
<td>Non-encrypted connections: http://[host]:[port]/activevos-central/avc</td>
</tr>
</tbody>
</table>

4. Verify that urn:mdm:service is mapped to the host name and port number of the MDM Hub Server:
   - Encrypted connections: https://[host]:[port]/cmx/services/BeServices
   - Non-encrypted connections: http://[host]:[port]/cmx/services/BeServices

Set the ActiveVOS Protocol to HTTPS

To enable secure communication between ActiveVOS and the MDM Hub, set the protocol to HTTPS in the Hub Console Workflow Manager.

You must first configure the application server for HTTPS communications.

1. Start the Hub Console.
2. Acquire a write lock.
3. Click Workflow Manager under the Configuration workbench.
4. In the Workflow Manager, click the Workflow Engines tab.
5. Select the ActiveVOS workflow engine, and then click the Edit button.
6. In the Edit Workflow dialog box, set the protocol to HTTPS.
7. In a WebLogic environment, in the Edit Workflow dialog box, enter the user name and password of the user that belongs to the abAdmin role.
Update Customized Workflows for Business Entities

If you have customized workflows that work with the business entities adapter, review the list of changes and make updates to your customized workflows as required.

The following table lists the changes that were made to the default workflows over the releases:

<table>
<thead>
<tr>
<th>Release</th>
<th>Change</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 HotFix 1</td>
<td>Enable password encryption.</td>
<td>For each workflow, set sif:encrypted to true.</td>
</tr>
<tr>
<td>10 HotFix 1</td>
<td>Update the presentation parameters for the task inbox.</td>
<td>&quot;Updating Presentation Parameters in Workflows for Business Entities&quot; on page 139</td>
</tr>
<tr>
<td>10.3</td>
<td>Enable the file attachments feature.</td>
<td>&quot;Enabling File Attachments in Workflows for Business Entities&quot; on page 141</td>
</tr>
</tbody>
</table>

Updating Presentation Parameters in Workflows for Business Entities

If you customized a workflow based on business entities, open the .bpel file and update the presentation parameters for each task.

The following table lists the updated presentation parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>hubUsername</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:hubUsername/text()</td>
</tr>
<tr>
<td>hubPassword</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:hubPassword/text()</td>
</tr>
<tr>
<td>securityPayload</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:securityPayload/text()</td>
</tr>
<tr>
<td>orsId</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:orsId/text()</td>
</tr>
<tr>
<td>taskTypeName</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:name/text()</td>
</tr>
<tr>
<td>taskTypeDisplayName</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:displayName/text()</td>
</tr>
<tr>
<td>taskTypeDescription</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:description/text()</td>
</tr>
<tr>
<td>pendingBVT</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:pendingBVT</td>
</tr>
<tr>
<td>taskTypeDataUpdateType</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:dataUpdateType/text()</td>
</tr>
<tr>
<td>taskTypeDisplayType</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:displayType/text()</td>
</tr>
<tr>
<td>defaultApproval</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/mdmavxsd:defaultApproval</td>
</tr>
<tr>
<td>Parameter</td>
<td>Expression</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>taskDataTaskId</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:taskId/text()</td>
</tr>
<tr>
<td>taskDataOwnerUID</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:ownerUID/text()</td>
</tr>
<tr>
<td>taskDataGroups</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:groups/mdmavxsd:groups/text()</td>
</tr>
<tr>
<td>dueDate</td>
<td>let $in := $ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:dueDate/text() let $out :=</td>
</tr>
<tr>
<td>status</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:status/text()</td>
</tr>
<tr>
<td>taskDataPriority</td>
<td>length($out) &gt; 0)), string-length($out) + (string-length($in )) * xsd:int((string-length($out) = 0))</td>
</tr>
<tr>
<td>taskDataSubjectAreaUID</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:subjectAreaUID/text()</td>
</tr>
<tr>
<td>taskDataTitle</td>
<td>let $in := $ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:title/text() let $out :=</td>
</tr>
<tr>
<td>taskDataComments</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:comments/text()</td>
</tr>
<tr>
<td>taskDataInteractionId</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:interactionId/text()</td>
</tr>
<tr>
<td>taskDataCreator</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:creator/text()</td>
</tr>
<tr>
<td>createDate</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:createDate</td>
</tr>
<tr>
<td>taskDataUpdatedBy</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:updatedBy/text()</td>
</tr>
<tr>
<td>lastUpdateDate</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:lastUpdateDate</td>
</tr>
<tr>
<td>beRowid</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:taskRecords/mdmavxsd:INFARecordKey[1]/mdmavxsd:rowId/text()</td>
</tr>
<tr>
<td>bePkeySrcObject</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:taskRecords/mdmavxsd:INFARecordKey[1]/mdmavxsd:pkeySrcObject/text()</td>
</tr>
<tr>
<td>beSystem</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:taskRecords/mdmavxsd:INFARecordKey[1]/mdmavxsd:system/text()</td>
</tr>
<tr>
<td>beRowidXref</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/mdmavxsd:taskRecords/mdmavxsd:INFARecordKey[1]/mdmavxsd:rowidXref/text()</td>
</tr>
<tr>
<td>Parameter</td>
<td>Expression</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>beTableUID</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskData/</td>
</tr>
<tr>
<td></td>
<td>mdmavxsd:taskRecords/mdmavxsd:INFAResultKey[1]/mdmavxsd:tableUID/text()</td>
</tr>
<tr>
<td>taskTypeCreationType</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/</td>
</tr>
<tr>
<td></td>
<td>mdmavxsd:creationType/text()</td>
</tr>
</tbody>
</table>

For more information about updating the .bpel files, see the ActiveVOS documentation.

Enabling File Attachments in Workflows for Business Entities

Effective in version 10.3, you can update your customized workflows to allow users to attach files to their tasks. To enable this feature in a customized workflow, update the process that initializes the data and update all the user processes.

**Note:** If you want to restrict the ability to add attachments to some tasks, you can configure the task settings in the Provisioning Tool. For more information about updating the task configuration, see the *Multidomain MDM Provisioning Tool Guide*.

1. In ActiveVOS Designer, open the .bpel file for a customized workflow.
   The workflow appears in the canvas.
2. Update the process that initializes the data.
   a. Select the Initialize Data process.
      The Operations dialog box appears.
   b. Click New Script.
      The Script Builder dialog box appears.
   c. In the Script box, add the following statement:
      \[
      \text{abx:copyAllAttachments('StartRequest', '_peopleActivityAttachments')}
      \]
      Replace StartRequest with the variable name that you use to initialize data in your workflow.
   d. Click OK.
      The Script Builder dialog box closes, and the script appears in the Operation list.
   e. Click OK.
      The Operations dialog box closes.
3. Update all the user processes.
   a. Select a user process.
   b. Click the Properties tab.
   c. Click the All tab.
   d. Expand Attachment Propagation.
   e. Set From Process to All.
   f. Set To Process to newOnly.
4. Save the .bpel file.
Configure the MDM Identity Services for ActiveVOS

If you use embedded ActiveVOS, ensure that you configure ActiveVOS to use MDM Identity Services. To configure the MDM Identity Services for ActiveVOS, use the ActiveVOS Console to set the Identity Services password to the password of the MDM Hub workflow engine user.

1. In the ActiveVOS console, select Admin > Configure Services > Identity Services.
2. In the Provider Configuration section, enable the Enable check box and select MDM from the Provider Type list.
3. In the Connection tab, enter the password of the MDM Hub user with the user name admin.
   Note: If you later change the password for the admin user, you must enter the new password in the ActiveVOS identity services settings.
4. Click Update.
5. Test that ActiveVOS can log in to the MDM Hub as the admin user, and that ActiveVOS can retrieve a list of roles for the user you specify as the User for test.
   a. Select the Test tab.
   b. In the User for test field, enter an MDM Hub user that is assigned to a role.
   c. Click Test Settings.
      Note: The test fails if an Operational Reference Store is not configured, the user for test does not belong to a role, or the role name contains spaces.

Custom BeMDMWorkflow Project (In-place Upgrade)

If you customized the workflows for the BeMDMWorkflow project, ensure that you update and then redeploy the project.

1. In Informatica ActiveVOS Designer, use the Project Explorer to navigate to BeCommonMDM > wsdl > cs.wsdl.
2. Right-click cs.wsdl, and then select Open With > Text Editor.
3. In the text editor, navigate to the following code:
   <xsd:complexType name="TaskFilter">
   <xsd:sequence>
4. Add the following code:
   <xsd:element minOccurs="0" name="overdueOnly" type="xsd:boolean" />
5. In Informatica ActiveVOS Designer, open the BeCommonMDM project to export.
6. Click File > Export.
   The Export dialog box opens.
8. In the Deployment URL field under Server Deployment Option, enter the URL for the ActiveVOS instance. Click Finish.
9. In the Deployment Complete dialog box, click OK.
Configure Unmerge and Merge Workflow Triggers (In-place Upgrade)

You must configure the unmerge and merge workflow triggers that were introduced in Multidomain MDM version 10.2. To configure the unmerge and merge workflow triggers, use the Provisioning tool.

For more information, see the Multidomain MDM Provisioning Tool Guide.

Add the Entity 360 Framework Task Manager

When you use the business entity ActiveVOS workflow adapter, you use the Entity 360 framework Task Manager and Entity 360 framework task inbox.

Update the Informatica Data Director configuration to replace the legacy task inbox. You can add the Entity 360 framework task inbox to the Home page. For more information about designing the Informatica Data Director user interface, see the Multidomain MDM Provisioning Tool Guide.
This chapter includes the following topics:

- **ActiveVOS Post-Upgrade Tasks for the Subject Area Adapter**, 144
- **Update the ActiveVOS URNs**, 144
- **Verifying the Trusted User for ActiveVOS**, 145
- **Update Informatica Data Director Task Configuration for ActiveVOS Workflows based on Subject Areas**, 145
- **Update Customized Workflows for Subject Areas**, 148
- **Redeploy the ActiveVOS Workflows based on Subject Areas**, 150
- **Generating Business Entity and Business Entity Services Configuration Files**, 150

### ActiveVOS Post-Upgrade Tasks for the Subject Area Adapter

Whether you perform a clean upgrade or an in-place upgrade, if you use the ActiveVOS workflow adapter based on subject areas, perform the ActiveVOS post-upgrade tasks for the subject area adapter to ensure your environment is properly configured.

### Update the ActiveVOS URNs

To use the HTTP Secure (HTTPS) protocol for secure communication between the MDM Hub and ActiveVOS, change the URLs in the URN paths from http to https.

1. Launch the ActiveVOS Console. In a browser, type the following URL, substituting the correct host name and port number:
   - **Secure connections**: https://<host>:<port>/activevos
   - **Non-secure connections**: http://<host>:<port>/activevos
2. In the ActiveVOS Console, on the Home page, click **Administration > Configure Server > URN Mappings**.
3. For the following URNs, update the paths to reflect the host name and port number of the ActiveVOS Server:

<table>
<thead>
<tr>
<th>URN</th>
<th>URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae:internal-reporting</td>
<td>Secure connections: https://&lt;host&gt;:&lt;port&gt;/activevos/internalreports</td>
</tr>
<tr>
<td></td>
<td>Non-secure connections: http://&lt;host&gt;:&lt;port&gt;/activevos/internalreports</td>
</tr>
<tr>
<td>ae:task-inbox</td>
<td>Secure connections: https://&lt;host&gt;:&lt;port&gt;/activevos-central/avc</td>
</tr>
<tr>
<td></td>
<td>Non-secure connections: http://&lt;host&gt;:&lt;port&gt;/activevos-central/avc</td>
</tr>
</tbody>
</table>

4. Verify that MDMHost:InfaMDM is mapped to the host name and port number of the MDM Hub Server:

| Secure connections: https://<host>:<port>/cmx/services/SifService |
| Non-secure connections: http://<host>:<port>/cmx/services/SifService |

### Verifying the Trusted User for ActiveVOS

In the Hub Console, verify that the ActiveVOS workflow engine settings specifies the trusted user.

1. In the Hub Console, on the Configuration workbench, click **Workflow Manager**.
2. Select the **Workflow Engines** tab.
3. Acquire a write lock.
4. Select **ActiveVOS** and click the **Edit** button.
5. In the Edit Workflow dialog box, enter the user name and password of the trusted user
6. Click **OK**.

### Update Informatica Data Director Task Configuration for ActiveVOS Workflows based on Subject Areas

To use the subject area-based ActiveVOS workflow adapter with the Task Manager, you must update the Informatica Data Director configuration file. If you use ActiveVOS workflows based on subject areas, you cannot migrate to ActiveVOS workflows based on business entities.

You can configure the following task parameters in the Informatica Data Director configuration file:

- **taskType**
  - Describes the task type.

- **taskTypeID**
  - The process name.

- **name**
  - The taskType name. The name must be the same as the name of the task in the ActiveVOS workflow configuration.
Update the IDD Configuration for the Subject Area-based ActiveVOS Adapter

To use the subject area-based ActiveVOS workflow adapter with the business entity-based Task Manager, update the Data Director configuration file. If you do not update the Data Director configuration file, you cannot use the Task Manager to create tasks.

The following code sample shows how to configure subject area-based ActiveVOS tasks in the Data Director configuration file for the workflows provided with Multidomain MDM:

```xml
<tasks includeUnassignedTasks="true">
  <!-- Task Definitions -->
  <taskType taskId="IDDMergeTask" name="AVOSMerge" displayName="Merge" creationType="MERGE" displayType="MERGE">
    <description>Merge two records together.</description>
  </taskType>

  <taskType taskId="IDDDUnmergeTask" name="AVOSUnmerge" displayName="Unmerge" creationType="UNMERGE" displayType="UNMERGE">
    <description>Unmerge an XREF record from a Base Object record.</description>
  </taskType>

  <taskType taskId="IDDOneStepApprovalTask" name="AVOSFinalReview" displayType="NORMAL" displayName="Final review" creationType="NONE" pendingBVT="true">
    <description>Update a record and require the user to go through an approval process before completing the task.</description>
  </taskType>

  <taskType name="Notification" displayName="Notification" creationType="NONE" displayType="NORMAL">
    <description>Notification step in the workflow.</description>
  </taskType>

  <taskType taskId="IDDTwoStepApprovalTask" name="AVOSReviewNoApprove" displayType="NORMAL" displayName="Review no approve" creationType="NONE" defaultApproval="true" pendingBVT="true">
    <description>Update a record and require the user to go through an approval process before completing the task.</description>
  </taskType>

  <taskType taskId="IDDDUpdateWithApprovalTask" name="Update" displayType="NORMAL" displayName="Update" creationType="CREATE" pendingBVT="true">
    <description>Update a record and do not require the user to go through an approval process before completing the task. The approval step is optional.</description>
  </taskType>
</tasks>
```

Configure Task Triggers For Subject Area Workflow Adapter

You must configure task triggers to use ActiveVOS workflows based on subject areas with the Task Manager. If you do not configure task triggers, the tasks do not appear in the Task Manager.

To configure triggers, use the Provisioning tool to edit the task configuration file from the Advance Configuration page. For more information, see the *Multidomain MDM Provisioning Tool Guide*.

You can configure the following `startWorkflow` attributes to configure task triggers:

- `process`
  - The name of the ActiveVOS workflow process.
taskKind

Defines the type of user interface required for the process. Can be REVIEW, MERGE, or UNMERGE. The taskKind is returned by the ActiveVOS workflow engine.

taskTemplate

The name of the task template to use.

firstTask Type

The first task in the workflow. Optional. This parameter allows the task to be assigned when the task is created.

Two-step approval code sample

The following code sample shows the startWorkflow element configuration for the ActiveVOS adapter based on subject areas for the two-step approval task:

```xml
<trigger name="DefaultApproval">
  <startWorkflow process="IDDTwoStepApprovalTask" taskKind="REVIEW" taskTemplate="Default Approval" firstTaskType="AVOSReviewNoApprove"/>
  <event name="CreateBE"/>
  <event name="UpdateBE"/>
  <role name="*"/>
</trigger>
```

One-step approval code sample

The following code sample shows the startWorkflow element configuration for the ActiveVOS adapter based on subject areas for the one-step approval task:

```xml
<trigger name="DefaultApproval">
  <startWorkflow process="IDDOneStepApprovalTask" taskKind="REVIEW" taskTemplate="Default Approval" firstTaskType="AVOSFinalReview"/>
  <event name="CreateBE"/>
  <event name="UpdateBE"/>
  <role name="*"/>
</trigger>
```

Update with approval code sample

The following code sample shows the startWorkflow element configuration for the ActiveVOS adapter based on subject areas for the update-with-approval task:

```xml
<trigger name="DefaultApproval">
  <startWorkflow process="IDDDUUpdateWithApprovalTask" taskKind="REVIEW" taskTemplate="Default Approval" firstTaskType="Update"/>
  <event name="CreateBE"/>
  <event name="UpdateBE"/>
  <role name="*"/>
</trigger>
```

Merge code sample

The following code sample shows the startWorkflow element configuration for the ActiveVOS adapter based on subject areas for the merge task:

```xml
<trigger name="Matched">
  <startWorkflow process="IDDMergeTask" taskKind="MERGE" taskTemplate="MergeTaskGenerator" firstTaskType="AVOSMerge"/>
  <event name="WatchedBE"/>
  <role name="SYSTEM"/>
</trigger>
```
Update Customized Workflows for Subject Areas

If you have customized workflows that work with the subject area adapter, review the list of changes and make updates to your customized workflows as required.

The following table lists the changes that were made to the default workflows over the releases:

<table>
<thead>
<tr>
<th>Release</th>
<th>Change</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 HotFix 1</td>
<td>Enable password encryption.</td>
<td>For each workflow, set $if:encrypted to true.</td>
</tr>
<tr>
<td>10 HotFix 1</td>
<td>Update the presentation parameters for the task inbox.</td>
<td>&quot;Updating Presentation Parameters in Workflows for Subject Areas&quot; on page 148</td>
</tr>
<tr>
<td>10.3</td>
<td>Enable the file attachments feature.</td>
<td>&quot;Enabling Attachments in Workflows for Subject Areas&quot; on page 149</td>
</tr>
</tbody>
</table>

Updating Presentation Parameters in Workflows for Subject Areas

If you customized a workflow based on subject areas, open the .bpel file and update the presentation parameters for each task.

The following table lists the updated presentation parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>subjectareauid</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:taskData/mdmavxsd:subjectAreaUID</td>
</tr>
<tr>
<td>title</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:taskData/mdmavxsd:title</td>
</tr>
<tr>
<td>creator</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:taskData/mdmavxsd:creator</td>
</tr>
<tr>
<td>mdmtasktype</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:taskType/mdmavxsd:name</td>
</tr>
<tr>
<td>orsId</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:orsId</td>
</tr>
<tr>
<td>duedate</td>
<td>string</td>
<td>$InfaTask/mdmavxsd:taskData/mdmavxsd:dueDate</td>
</tr>
<tr>
<td>tasktypename</td>
<td>string</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/name</td>
</tr>
<tr>
<td>taskTypeDisplayName</td>
<td>string</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/displayName</td>
</tr>
<tr>
<td>taskTypeDescription</td>
<td>string</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/description</td>
</tr>
<tr>
<td>taskTypePendingBVT</td>
<td>boolean</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/pendingBVT</td>
</tr>
<tr>
<td>taskTypeDataUpdateType</td>
<td>string</td>
<td>$ProcessTaskRequest/mdmavxsd:INFATask/mdmavxsd:taskType/dataUpdateType</td>
</tr>
</tbody>
</table>
**Enabling Attachments in Workflows for Subject Areas**

Effective in version 10.3, you can update your customized workflows to allow users to attach files to their tasks. To enable this feature in a customized workflow, update the process that initializes the data and update all the user processes.

**Note:** If you want to restrict the ability to add attachments to some tasks, you can configure the task settings in the Provisioning Tool. For more information about updating the task configuration, see the *Multidomain MDM Provisioning Tool Guide*.

1. In ActiveVOS Designer, open the .bpel file for a customized workflow.
   
   The workflow appears in the canvas.

2. Update the process that initializes the data.
   
   a. Select the **Initialize Data** process.
      
      The **Operations** dialog box appears.
   
   b. Click **New Script**.
      
      The **Script Builder** dialog box appears.
   
   c. In the **Script** box, add the following statement:  
      
      ```
      abx:copyAllAttachments('StartRequest', '_peopleActivityAttachments')
      ```
      
      Replace StartRequest with the variable name that you use to initialize data in your workflow.
   
   d. Click **OK**.
      
      The **Script Builder** dialog box closes, and the script appears in the **Operation** list.
   
   e. Click **OK**.
      
      The **Operations** dialog box closes.

3. Update all the user processes.
   
   a. Select a user process.
   
   b. Click the **Properties** tab.
   
   c. Click the **All** tab.
   
   d. Expand **Attachment Propagation**.
   
   e. Set **From Process** to **All**.
   
   f. Set **To Process** to **newOnly**.

4. Save the .bpel file.
Redeploy the ActiveVOS Workflows based on Subject Areas

The ActiveVOS workflows for the workflow adapter that is based on subject areas changed in version 10.0 HotFix 2. If you use the workflow adapter based on subject areas, you must redeploy the default workflows that are provided in the Resource Kit. To deploy the Informatica ActiveVOS project that contains the task workflows to the MDM Hub Server, first export the CommonMDM project and then export the MDMWorkflow project.

1. In Informatica ActiveVOS Designer, open the BeCommonMDM project to export.
2. Click File > Export.
   The Export dialog box opens.
4. In the Deployment URL field under Server Deployment Option, enter the URL for the ActiveVOS instance. Click Finish.
5. In the Deployment Complete dialog box, click OK.
6. Repeat all steps for the BeMDMWorkflow project.
   You must export the BeCommonMDM project before you export the BeMDMWorkflow project.

Generating Business Entity and Business Entity Services Configuration Files

To generate business entity and business entity services configuration files, use the Informatica Data Director Configuration Manager.

1. In the Configuration Manager Applications pane, select the Informatica Data Director application whose configuration you want to generate into a business entity and business entity service configuration.
2. Click Generate Business Entity Schema.
   Configuration Manager generates the business entity and business entity service configuration.
3. Configuration Manager displays messages of issues encountered while generating the business entity and business entity services configuration. The messages indicate if Configuration Manager resolved the issue during the generation process and describes the changes Configuration Manager made to resolve the issue. If Configuration Manager did not fix the issue, note the issue and the suggested action you can take to resolve the issue.
Appendix A

Troubleshooting the Upgrade Process

If the upgrade fails or you encounter issues during the upgrade, use the following information to troubleshoot the problem.

The EAR files do not deploy within the permitted time in JBoss environments.

As you increase the number of Operational Reference Stores, the EAR file deployment time increases. If the EAR file deployment time exceeds the permitted deployment time in JBoss environments, the upgrade fails.

To resolve the issue, increase the permitted deployment time to accommodate the EAR file deployment time. The default permitted deployment time is 600 seconds.

1. Increase the value of the `deploy.wait.time` property in the `build.properties` file in the following directory: `<infamdm installation directory>/hub/server/bin`

2. Navigate to the following directory: `<JBoss installation directory>/standalone/configuration`

3. Configure the following code in the `standalone-full.xml` file to increase the timeout value:

   ```xml
   <subsystem xmlns="urn:jboss:domain:deployment-scanner:1.1">
     <deployment-scanner path="deployments" relative-to="jboss.server.base.dir" scan-interval="5000" deployment-timeout="1200"/>
   </subsystem>
   ```

The Hub Server upgrade fails.

To resolve the issue, redeploy the EAR file to retry the Hub Server upgrade.

**Note:** In JBoss environments, if you manually change the configuration of data sources in the `standalone-full.xml` file when JBoss is running, you lose the configuration changes when you run the `patchInstallSetuup` script.

1. Navigate to the following directory: `<MDM Hub installation directory>/hub/server`

2. Run the following command to deploy the Hub Server application and apply changes to the application server configuration.

   **Note:** If you do not have embedded ActiveVOS in your environment, you do not need to include the ActiveVOS user names and passwords in the command.

**On UNIX**

```
patchInstallSetuup.sh -Dweblogic.password=<WebLogic password> -Ddatabase.password=<MDM Hub Master database password> -Davos.username=<ActiveVOS
```
When you upgrade the Process Server in a WebLogic environment, the upgrade might fail with the following error:

```
Unable to start application, deployment error msg: weblogic.management.ManagementException: [Deployer:149196]Rejecting start request for application siperian-mrm-cleanae.ear because stop request is running for the application.
```

To resolve the issue, use the WebLogic Administrative Console to manually deploy the `siperian-mrm-cleanae.ear` file, and then restart the application server.

**The Process Server upgrade fails in a WebLogic environment.**

When you upgrade the Process Server in a WebLogic environment, the upgrade might fail with the following error:

```
Unable to start application, deployment error msg: weblogic.management.ManagementException: [Deployer:149196]Rejecting start request for application siperian-mrm-cleanae.ear because stop request is running for the application.
```

To resolve the issue, use the WebLogic Administrative Console to manually deploy the `siperian-mrm-cleanae.ear` file, and then restart the application server.
The Process Server upgrade fails.

To resolve the issue, redeploy the EAR file to retry the Process Server upgrade.

**Note:** If you manually change the configuration of data sources in the standalone-full.xml file when JBoss is running, you lose the configuration changes when you run the `patchInstallSetup` script.

1. **Navigate to the following directory:** `<MDM Hub installation directory>/hub/cleanse`
2. **Run the following command to deploy the Process Server application and apply changes to the application server configuration.**

   **On UNIX**
   - WebLogic
     ```bash
     patchInstallSetup.sh -Dweblogic.password=<WebLogic password> -Ddatabase.password=<your database password>
     ```
   - WebSphere
     ```bash
     patchInstallSetup.sh -Ddatabase.password=<your database password>
     ```
   - JBoss
     ```bash
     patchInstallsetup.sh -Ddatabase.password=<your database password>
     ```

   **On Windows**
   - WebLogic
     ```bash
     patchInstallSetup.bat -Dweblogic.password=<WebLogic password> -Ddatabase.password=<your database password>
     ```
   - WebSphere
     ```bash
     patchInstallSetup.bat -Ddatabase.password=<your database password>
     ```
   - JBoss
     ```bash
     patchInstallsetup.bat -Ddatabase.password=<your database password>
     ```

   **Note:** On UNIX, if you include an exclamation mark (!) character in the password, you must include a backslash before the exclamation mark (!) character. For example, if the password is `!!cmx!!`, enter `\!!cmx\!!`.

The Informatica Platform Upgrade fails.

To confirm that the Informatica platform installed successfully, see the following Knowledge Base article: [https://kb.informatica.com/faq/7/Pages/14/306938.aspx?myk=KB%20306938](https://kb.informatica.com/faq/7/Pages/14/306938.aspx?myk=KB%20306938).

To troubleshoot the Informatica platform installation if it was not successful, see the following Knowledge Base article: [https://kb.informatica.com/faq/7/Pages/14/306941.aspx?myk=KB%20306941](https://kb.informatica.com/faq/7/Pages/14/306941.aspx?myk=KB%20306941).

When I upgrade an Operational Reference Store, Oracle generates error ORA-20005.

If you encounter error ORA-20005 when you run `sip_ant updateorsdatabase`, perform the following steps:

1. **Run the following command to grant the required permissions:**
   ```bash
   exec dbms_java.grant_permission('ORS_USER','SYS:java.net.SocketPermission','connect,resolve');
   ```

2. **Run the following command to confirm that the Java classes are loaded in Oracle:**
   ```sql
   select dbms_java.longname(object_name), status from user_objects where object_type='JAVA CLASS';
   ```
3. If the classes are not loaded, run the following command to reload the classes:

```bash
loadjava -verbose -force -resolve -oracleresolver -user &ors_name/
&ors_password@&tns_name siperian-cleansecaller.jar
loadjava -verbose -force -resolve -oracleresolver -user &ors_name/
&ors_password@&tns_name siperian-dutil.jar
```

The Hub Store upgrade fails.
You cannot rerun the Hub Store upgrade on a partially upgraded schema. If the upgrade fails, restore the
database from a full backup, and then rerun the Hub Store upgrade.

If the Hub Store upgrade fails because column names contain reserved words, contact Informatica Global
Customer Support for scripts to migrate the data to renamed columns.

After upgrading from a non-English locale, some tables are in English and some are in the
language of the locale.
If your Hub Store database environment is set to a non-English locale, you must change the character set to
Unicode before you run the upgrade scripts to upgrade the MDM Hub Master Database and Operational
Reference Stores. During the upgrade, all table metadata is translated to English with a translation key. If you
did not select a Unicode character set, only some tables are translated.

Hub Console fails to launch
Verify that you are using a Java runtime environment (JRE) that is supported for the Hub Console. For system
requirements, see the Product Availability Matrix for this version of Multidomain MDM on Informatica
Network:

The Hub Console fails to launch in a JBoss environment
In JBoss environments, if the JBoss application server does not restart, you cannot launch the Hub Console.
The MDM Hub generates an error to indicate that the repository layer did not initialize.
To resolve the issue, run the following code in a batch file to restart JBoss:

```bash
rmdir C:\<JBoss installation directory>\standalone\tmp /s /q
mkdir C:\<JBoss installation directory>\standalone\tmp
C:\<JBoss installation directory>\bin\standalone.bat -c standalone-full.xml -b 0.0.0.0
```

Hub Console fails to launch in a DB2 environment
In an MDM Hub environment with DB2 datasources, the Hub Console fails to launch with the following errors:

**SIP-09070:** SIP-10318: Couldn't get users due to data access error.

**SIP-10324:** There was an unexpected exception when attempting to load data object(s).
java.lang.NullPointerException

This issue is caused by a mismatch in the case used for the administrative user name in the MDM Hub and in
the application server. For example, the MDM Hub has the administrative user DB2ADMIN (uppercase) while
the application server has db2admin (lowercase).

To resolve the issue, ensure that the user name in the application server exactly matches the user name in
the MDM Hub.

**Note:** To avoid issues related to case-sensitivity, Informatica recommends using all uppercase letters when
defining user names for DB2.

For example, if you are using WebSphere, set the user name in the WebSphere Console.
1. Open the WebSphere Console.
2. Navigate to Resources > Data sources > siperian-cmx_system-ds > Custom properties.
3. In the User field, type in uppercase: DB2ADMIN
4. In the Password field, type the password for this user.
5. Click Apply, and then click Save.
6. Restart WebSphere.
7. Launch the Hub Console and log in.

In IDD, users cannot use the legacy Data View to view records that are based on subject areas. The default page to view records in IDD is the Entity View that is based on business entities.

To use the legacy Data View, set `dataview.enabled=true` in the cmxserver.properties file.

For more information, see the following How-to article: Migrating IDD Applications to the Business Entity Data Model.

**IDD fails with the error SIP-BV-11500.**

IDD can fail with the following error: SIP-BV-11500 Fatal Error Operational Reference Store localhost-orcl-MDM_SAMPLE does not have a workflow engine configured. Each Operational Reference Store must have a workflow engine configured for use with the IDD even if workflow will not be used.

To resolve this issue, ensure that the primary workflow adapter is configured.

For more information, see the following KB article: https://kb.informatica.com/solution/23/Pages/55/381456.aspx?myk=381456.

When you validate the metadata, an error states that the object exists in the metadata but not in the database.

When you use the Repository Manager to fix the issue, the following error occurs: ORA-00955 Name is already used by an existing object.

To resolve the issue, ensure that the correct privileges for the proxy role are granted for the tables that encounter the error. Refer to a table that does not encounter the error to get the list of permissions that are required.

**On Windows, when match tokens are generated, an error occurs.**

The Generate Match Tokens process returns an error that says that the class `ssa.ssaname3.jssan3cl` cannot be initialized.

1. Verify that the PATH environment variable includes the path to the following directory, which contains the dynamic linked library (DLL) files for SSA-NAME3: <MDM installation directory>/hub/cleanse/lib
3. If Microsoft Visual C++ Redistributable for Visual Studio 2015 is installed, use a dependency checker, such as Dependency Walker (depends.exe), to load jssan3cl.dll and confirm that the Visual C++ Redistributable was successfully applied.

   **Tip:** Visual C++ Redistributable for Visual Studio 2015 requires that Windows Server has operating system patches installed. Check the operating system requirements before installing Visual C++ Redistributable. For example, from a baseline version of Windows Server 2012, you must apply around 100 patches (totalling approximately 2 GB) to the operating system before you can successfully install Visual C++ Redistributable.

After you upgrade in a Microsoft SQL Server environment on a WebLogic application server, you cannot log in to the Hub Console.

A null pointer exception occurs when you log in to the Hub Console.

To resolve the issue, comment out the drop commands, create schema commands, and any role commands in the `xa_install.sql` script located in `<Microsoft SQL Server installation directory>\sqljdbc_4.0\enu\xa`. Run the script, and then restart the application server.

The upgrade component `patchInstallSetup` fails when you install the Hub Server on a WebSphere Application Server.

To resolve the issue, open the file `<WebSphere profile home>/properties/soap.client.props` and increase `com.ibm.SOAP.requestTimeout`, and then restart the WebSphere server profile. Run `patchInstallSetup.bat` again.

The `entity360view.ear` file fails to deploy when you upgrade the Hub Server in IBM AIX environments.

To resolve the issue, run the `patchInstallSetup.sh` script.
Frequently Asked Questions

Do we need a new license file to upgrade?
Yes. If you are upgrading from a Multidomain MDM version 10.1.x or earlier, you need a new license file.

Can we use database user exits from a pre-10.0 version?
No. Database user exits that run in the database layer are deprecated in version 10.0 and later.

Why do we need to provide the DBA username and password during the upgrade process?
The upgrade process performs actions that require DBA-level permissions, such as granting privileges and creating sequences. The DBA credentials are necessary to allow the upgrade process to perform these actions.

What happens to the existing version of ActiveVOS during the upgrade process?
If you have ActiveVOS installed in your environment and you do an in-place upgrade, the upgrade process will install the latest version of ActiveVOS if your environment does not already have it. To see which version of ActiveVOS is required, see the Product Availability Matrix on Informatica Network:

Is it mandatory to install ActiveVOS during the MDM upgrade process in an environment that does not have ActiveVOS installed?
No. During the upgrade process, you are prompted to choose whether you want to install ActiveVOS.

Has the recommended screen resolution for Informatica Data Director changed in this version?
No, the recommended screen resolution has not changed. The recommended screen resolution for Informatica Data Director is 1280 x 1024.

Do we need to upgrade Informatica Data Quality when we upgrade to Multidomain MDM version 10.2 or later?
Yes, if you use Informatica Data Quality (IDQ) in your environment, you must upgrade to version 10.1 of IDQ. For the system requirements, see the Product Availability Matrix on Informatica Network:

How do we customize MDM Hub security?
For information about customizing MDM Hub security, see the Multidomain MDM Security Guide and see the How-to article Using the Security Configuration Utility in Multidomain MDM.

Is Java 8 supported?
Yes, this version of Multidomain MDM supports Java 8. For the system requirements, see the Product Availability Matrix on Informatica Network:
Note: ActiveVOS requires Java 7.

If we do not install the Informatica platform, why is the Informatica platform EAR file deployed?
The Informatica platform EAR is deployed to enable the MDM Hub to communicate with the platform. If the Informatica platform is not installed, the EAR file is deployed as a passive application.

If we migrate to use Informatica platform staging, can we set up delta detection, hard delete detection, and audit trails?
By default, Informatica platform staging does not include support for these features. Build your own customization outside the MDM Hub to provide these functions.
APPENDIX C

Processing Existing ActiveVOS Tasks

This appendix includes the following topics:

- Processing Existing ActiveVOS Tasks Overview, 159
- Migration Properties, 159
- Running the Migration Script with a Properties File, 160
- Running the Migration Script with Properties on the Command Line, 161

Processing Existing ActiveVOS Tasks Overview

To work with ActiveVOS tasks that were created before Multidomain MDM version 10.1, routinely run a migration script to populate the tasks with the required presentation parameters. If you do not run the migration script, the tasks do not appear in the Task Manager. Run the migration script until you process all the tasks that were created before you upgraded to version 10.1.

The migration script requires that you set some properties. You can add the properties to a build file or you can add them in the command line.

Migration Properties

The following table describes the migration properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>avos.jdbc.database.driver.jar</td>
<td>Path to the JAR file that contains the JDBC driver for ActiveVOS database.</td>
</tr>
<tr>
<td></td>
<td>This parameter is populated during the Hub Server installation without the avos</td>
</tr>
<tr>
<td></td>
<td>prefix in &lt;infamdm installation directory&gt;\conf\avos.install.properties.</td>
</tr>
<tr>
<td>avos.jdbc.database.driver.class</td>
<td>JDBC driver class for ActiveVOS database.</td>
</tr>
<tr>
<td></td>
<td>This parameter is populated during the Hub Server installation without the avos</td>
</tr>
<tr>
<td></td>
<td>prefix in &lt;infamdm installation directory&gt;\conf\avos.install.properties.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>avos.jdbc.database.url</td>
<td>ActiveVOS database connection URL. This parameter is populated during the Hub Server installation without the avos prefix in <code>&lt;infamdm installation directory&gt;/conf/avos.install.properties</code>.</td>
</tr>
<tr>
<td>avos.jdbc.database.username</td>
<td>ActiveVOS database user name. This parameter is populated during the Hub Server installation without the avos prefix in <code>&lt;infamdm installation directory&gt;/conf/avos.install.properties</code>.</td>
</tr>
<tr>
<td>avos.jdbc.database.password</td>
<td>ActiveVOS database password.</td>
</tr>
<tr>
<td>avos.ws.protocol</td>
<td>The protocol for the ActiveVOS server connection. Can be http or https.</td>
</tr>
<tr>
<td>avos.ws.host</td>
<td>Host name of the application server where ActiveVOS runs.</td>
</tr>
<tr>
<td>avos.ws.port</td>
<td>Port number of the application server connection.</td>
</tr>
<tr>
<td>avos.ws.trusted.username</td>
<td>User name of the trusted user. <strong>Note:</strong> The trusted user is created as part of the Multidomain MDM installation and upgrade process.</td>
</tr>
<tr>
<td>avos.ws.trusted.password</td>
<td>Password for the trusted user. <strong>Note:</strong> The trusted user is created as part of the Multidomain MDM installation and upgrade process.</td>
</tr>
<tr>
<td>avos.hub.username</td>
<td>MDM Hub super user that belongs to all task management roles.</td>
</tr>
<tr>
<td>avos.ws.pagesize</td>
<td>Number of tasks processed in one database transaction and batch-loaded from ActiveVOS.</td>
</tr>
<tr>
<td>avos.ws.statuses</td>
<td>Optional. Comma-separated list of ActiveVOS task statuses to be processed. For example, READY or IN_PROGRESS. By default all tasks are processed.</td>
</tr>
</tbody>
</table>

**Running the Migration Script with a Properties File**

Create an MDM user that belongs to the roles associated with the workflows. Add the migration properties to the Hub Server `build.properties` file, and then run the MDM Hub Master Database with the migration script command. After the migration, task owners can continue to take action on their assigned tasks.

Run the migration script on a regular schedule. After all the tasks for the subject area workflow adapter are processed, you no longer have to run the script and you can delete the MDM user that you created for this purpose.

1. Create an MDM Hub user, and assign the user all the roles that participate in workflows.
   For example, the predefined workflows use the following roles: DataSteward, Manager, and SrManager.

2. Open the following file in a text editor:
   `<MDM Hub installation directory>/hub/server/bin/build.properties`

3. Add the migration properties to the `build.properties` file. For a list of properties, see "Migration Properties" on page 159.

4. Open a command prompt.
Running the Migration Script with Properties on the Command Line

Create an MDM user that belongs to the roles associated with the workflows. Open a command prompt and run the script with the desired properties. After the migration, task owners can continue to take action on their assigned tasks.

Run the migration script on a regular schedule. After all the tasks for the subject area workflow adapter are processed, you no longer have to run the script and you can delete the MDM user that you created for this purpose.

1. Create an MDM Hub user, and assign the user all the roles that participate in workflows. For example, the predefined workflows use the following roles: DataSteward, Manager, and SrManager.

2. Open a command prompt.

3. Navigate to the following directory:

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

4. Run the MDM Hub Master Database upgrade script with the migration script command and the migration properties. For a list of properties, see "Migration Properties" on page 159.

   For example, you can run one of the following commands:

   - On UNIX.

     ```bash
     sip_ant.sh migrate-avos=sa-tasks -Davos.jdbc.database.password=!cmx!!
     -Davos.ws.protocol=http -Davos.ws.host=localhost -Davos.ws.port=8080 -
     Davos.ws.pageSize=100
     -Davos.ws.trusted.username=avos -Davos.ws.trusted.password=avos -
     Davos.hub.username=admin
     ```

   - On Windows.

     ```cmd
     sip_ant.bat migrate-avos=sa-tasks -Davos.jdbc.database.password=!cmx!!
     -Davos.ws.protocol=http -Davos.ws.host=localhost -Davos.ws.port=8080 -
     Davos.ws.pageSize=100
     -Davos.ws.trusted.username=avos -Davos.ws.trusted.password=avos -
     Davos.hub.username=admin
     ```
Configuring Metadata Caching

This appendix includes the following topic:

- Configuring Metadata Caching (Optional), 162

Configuring Metadata Caching (Optional)

The metadata caches manage items such as data objects, repository objects, and search tokens. The MDM Hub uses Infinispan for metadata caching. Infinispan is installed with the Hub Server. For the caches that are used by the Hub Server, the Infinispan configuration file contains default attribute values.

In version 10.1 and earlier, the MDM Hub used JBoss Cache for metadata caching. After you upgrade from one of these versions, the MDM Hub Server uses the Infinispan configuration file instead of the JBoss Cache configuration file.

If the JBoss Cache configuration file was edited in the previous version of MDM Hub, you might need to edit the Infinispan configuration file. It depends on why the file was edited.

Network policy

If the JBoss Cache file was edited to work around your organization’s network policy, update the Infinispan file and the jgroups* file with the same policy changes.

Performance

If the JBoss Cache file was edited to improve cache performance, first try running the MDM Hub with the default Infinispan values. If you experience performance issues, copy the changed values from the JBoss Cache configuration file to the Infinispan configuration file. If you still experience performance issues, familiarize yourself with Infinispan and adjust the values to better suit your environment.
Infinispan Attributes

The following table summarizes default Infinispan attribute values and indicates how the attributes map to the former JBoss attribute:

<table>
<thead>
<tr>
<th>Infinispan Element and Attribute</th>
<th>Default Value</th>
<th>Description</th>
<th>JBoss Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>locking acquire-timeout</td>
<td>60000</td>
<td>Maximum time during which the Hub Server can try to acquire a lock.</td>
<td>lockAcquisitionTimeout</td>
</tr>
<tr>
<td>transaction stop-timeout</td>
<td>30000</td>
<td>When a cache stops, this attribute sets the maximum time that Infinispan waits while the Hub Server finishes remote and local transactions.</td>
<td>sync replTimeout</td>
</tr>
<tr>
<td>transport cluster</td>
<td>infinispan-cluster</td>
<td>Name for the underlying group communication cluster.</td>
<td>clustering</td>
</tr>
<tr>
<td>transport stack</td>
<td>UDP</td>
<td>Type of configuration: UDP or TCP. The configurations are defined in the jgroups-udp.xml file and the jgroups-tcp.xml file.</td>
<td>jgroupsConfig</td>
</tr>
<tr>
<td>transport node-name</td>
<td>$node$</td>
<td>Name of the current node. The Hub Server sets this attribute. The node-name defaults to a combination of the host name and a random number. The number differentiates multiple nodes on the same host.</td>
<td>--</td>
</tr>
<tr>
<td>transport machine</td>
<td>$machine$</td>
<td>ID of the machine where the node runs. The Hub Server sets this attribute.</td>
<td>--</td>
</tr>
<tr>
<td>expiration lifespan</td>
<td>--</td>
<td>Maximum lifespan of a cache entry in milliseconds. When a cache entry exceeds its lifespan, the entry expires within the cluster. If you need to optimize performance, increase the lifespan for the following caches: DISABLE_WHEN_LOCK, DATA_OBJECTS, and REPOS_OBJECTS. For example, you can increase the lifespan from one hour (3600000) to one day (86400000). Each cache has its own default value for this attribute. To find the default values, open the inifinspanConfig.xml file.</td>
<td>eviction timeToLive</td>
</tr>
<tr>
<td>expiration interval</td>
<td>--</td>
<td>Maximum interval for checking the lifespan. If you need to optimize performance, increase the interval for the following caches: DISABLE_WHEN_LOCK, DATA_OBJECTS, and REPOS_OBJECTS. For example, you can increase the interval from five seconds (5000) to five minutes (300000). Each cache has its own default value for this attribute. To find the default values, open the inifinspanConfig.xml file.</td>
<td>eviction timeToLive</td>
</tr>
</tbody>
</table>
Editing Infinispan Attributes

To configure metadata caching attributes, edit the `infinispanConfig.xml` file for the Hub Server. For help with the Infinispan configuration, see the Infinispan documentation.

**Note:** The Process Server also has an Infinispan configuration file. The default attribute values should be sufficient, however if you notice issues with the performance of the Process Server, you can fine-tune the attribute values.

1. **Navigate to the following directory:** `<MDM Hub installation directory>/hub/server/resources`
2. **Make a backup copy of the following file:** `infinispanConfig.xml`
3. **Open the `infinispanConfig.xml` file and find the Infinispan version number, which appears in the `xsi:schemaLocation` attribute.**
4. **Review the documentation for the Infinispan version.**
   
   **Note:** In the following URLs, substitute the version number wherever the path contains `#.#`.  
   - To view the configuration schema, go to the URL that is contained in the `xsi:schemaLocation` attribute in the file.
   - To learn about the attributes, go to `https://docs.jboss.org/infinispan/<#.x>/configdocs/`
   - To learn about Infinispan, go to `http://infinispan.org/docs/<#.x>/` and select the "Frequently Asked Questions" link.
5. **Edit the file and save it.**
INDEX

A
ActiveVOS
   silent installer properties 84
   URN, setting 138, 144
ActiveVOS Console administrative user
   abAdmin role 48, 53, 62
   attachments
      enabling in custom workflows 141
      enabling, in workflows for subject areas 149

C
cmxserver.log file 86, 97
   configuring IBM DB2
      for the MDM Hub 37
   configuring JBoss
      for the MDM Hub 44
   configuring Microsoft SQL Server
      for the MDM Hub 33
   configuring Oracle
      disable the Oracle Recycle Bin 27
      for the MDM Hub 27
   set the init.ora parameters 27
   configuring WebSphere
      for Informatica Data Director 68
      custom code, testing 119

D
Data Director
   upgrade tests 120
      upgrade tests for subject areas 120
   database
      create manually 38
      databases
         connection testing 27

E
elasticsearch archive
   extracting 124
   environment report
      review 117
      saving 117

F
file attachments
   enabling in custom workflows 141
   enabling, in workflows for subject areas 149

H
Hub Server
   reapplying the upgrade 87
   silent properties file 84
   silent upgrade 83, 85
   upgrading in graphical mode 78
Hub Server upgrade
   about 77
   console mode 91
   Hub Server upgrades
      log files 86
   Hub Store
      tablespaces, creating 27, 37
   Hub Store upgrade
      about 69
      Operational Reference Store
         upgrade 72
   Hub Store upgrades
      Master Database 70
      hub_cleanse_install.bin 88
      hub_cleanse_install.exe 88
      hub_install.bin 78
      hub_install.exe 78

I
infamdm_installer_debug.txt file 86, 97
   Infinispan
      configuring 164
   Informatica ActiveVOS
      creating the schema 30, 34, 41

J
Java options
   configuring 59
   JBoss
      starting on JBoss cluster nodes 50
      starting on standalone JBoss instances 49
   JBoss starting on cluster nodes
      starting on standalone instances 49
   JVM parameters
      configuring 59

L
log files
   application server log files 86, 97
   Cleanse Match Server upgrades 97
   cmxserver.log file 86, 97
   Hub Server upgrades 86
   Infamdm_Cleanse_Match_Server_InstallLog.xml file 97
log files (continued)
infadm_installer_debug.txt file 86, 97
Infadm_Server_InstallLog.xml file 86
postInstallSetup.log file 86, 97

M
match population
   enabling 95
MDM Hub
   upgrade tests 119
MDM Hub Master Database upgrade
   silent mode 71
   verbose mode 70
metadata
   validating 115, 116
   validation messages, resolving 116
metadata validation
   validation checks 116
Microsoft SQL Server
   configuring 33
   data file store 34
   distributed transactions 33
   installing 33
   ODBC Driver 34
   unixODBC Driver 34

O
Operational Reference Store
   registering 21
Operational Reference Store upgrade
   silent mode 75
   verbose mode 72

P
postInstallSetup.log file 86, 97
preface 9
Process Server
   reapplying the upgrade 98
   silent properties file 92
   silent upgrade 92
   upgrading in console mode 90
   upgrading in graphical mode 88
Process Server upgrades
   about 88
   log files 97

R
Resource Kit
   uninstalling 99
   upgrading 99

S
search
   stopwords 129
   stopwords.txt file 129
   synonyms 130
   synonyms.txt file 130
   words to ignore 129
   silent upgrade of Hub Server 85
   running the Process Server silent upgrade 93
stopwords.txt file
   customizing 129
synonyms.txt file
   customizing 130

tablespace
   creating 27, 37
   testing
      custom code 119
      tests
      upgrade tests 118
      tns name
      adding 27
   troubleshooting
      post-installation process 151
   
U
uninstalling
   Resource Kit 99
upgrade
   Master Database 70
   upgrade process
      clean upgrade 12
      in-place upgrade 13
   upgrade tests
      about 118
      Data Director with business entities 120
      Data Director with subject areas 120
      Hub Console tools 119
      Provisioning tool 119
   upgrading
      guidelines 12
      overview 11, 12
      restarting environment 106
URN
   setting ActiveVOS 138, 144
   
V
validation results
   saving 116

W
WebLogic
   configuring 50
WebSphere
   configuring 58
WebSphere administrative security
   running the Hub Server PostInstallSetup script 109
   running the Process Server PostInstallSetup script 110
uninstalling the EAR files 108
WebSphere security
   unregistering the ORS 108
workflows
   custom, enabling file attachments 141
   workflows for subject areas
      custom, enabling file attachments 149