

Oracle Metadata Management (OMM) Solutions

Oracle Metadata Management for Oracle Business Intelligence (OMM4OBI)
Oracle Enterprise Metadata Management (OEMM)

OMM Metadata Management

with Meta Integration® Metadata Management (MIMM)

README for Release Notes, Installation & Setup

Table of Contents

1	Overview
2	Copyright Notice
3	Release Changes
4	System requirements
5	Database Server Setup
5.1	Database on Oracle
6	Application Server Setup
6.1	Application Server Installation and Configuration
6.2	Application Server Upgrade
6.3	Application Server Execution and Initialization
6.4	Custom integration with Authentication Environments
6.5	Custom integration for Secure Socket Layer (SSL) communication
6.6	Security and Vulnerability Considerations
7	Metadata Harvesting Model Bridge (MIMB) Setup
8	User Interface Look & Feel Customization
8.1	Login and Headers
8.2	Metadata Explorer for Business Users
9	REST API SDK
10	Database Server Backup/Restore
10.1	Database on Oracle

1. Overview

The Oracle Metadata Management (OMM) solutions include two products:

- the Oracle Metadata Management for Oracle Business Intelligence (OMM4OBI)
- and the Oracle Enterprise Metadata Management (OEMM)

Oracle Metadata Management for Oracle Business Intelligence is a software package for metadata management of Oracle environments. Oracle Metadata Management for Oracle Business Intelligence includes the following metadata management features:

- Metadata Harvesting from Oracle technologies
- Metadata Configuration and Stitching
- Metadata Browsing, Search and Reporting
- Metadata Collaboration (external URL, tagging, comments and review)
- Data Flow Lineage & Impact Analysis
- Metadata Explorer (simplified metadata user interface for business users)

Oracle Enterprise Metadata Management is a software package for metadata management of multi-vendor environments and support for data governance. Oracle Enterprise Metadata Management includes all features of Oracle Metadata Management for Oracle Business Intelligence with the following extra metadata management features:

- Metadata Harvesting from multi-vendor technologies
- Metadata Version and Configuration Management (change management)
- Data Model Diagram Visualizer and Navigator
- Business Glossary for Data Governance
- Semantic Lineage & Impact Analysis
- Semantic Mapping Editor
- Data Flow Mapping Specifications Editor

The above Oracle Metadata Management Solutions are implemented by Meta Integration® Metadata Management (MIMM) Web Application Server, based on a Meta Integration® Repository (MIR) database server, and the Meta Integration® Model Bridge (MIMB) metadata harvesting components.

2. Copyright Notice

The following Oracle Metadata Management (OMM) products:

- Oracle Metadata Management for Oracle Business Intelligence (OMM4OBI)
- Oracle Enterprise Metadata Management (OEMM)

are licensed under the following Oracle copyright:

Copyright © 2014-2018, Oracle and/or its affiliates.
All Rights Reserved.

The Oracle logo and Oracle product names referenced herein are either registered trademarks or trademarks of Oracle and/or its affiliates. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Oracle® is a registered trademark of Oracle.

These Oracle Metadata Management products are based (re-branded OEM) on the following Meta Integration products:

- Meta Integration® Metadata Management (MIMM)
- Meta Integration® Model Bridge (MIMB)
- Meta Integration® Repository (MIR)

which are licensed under the following Meta Integration copyright:

Copyright © Meta Integration Technology, Inc. 1997-2018.
All Rights Reserved.
Meta Integration® is a registered trademark of Meta Integration Technology, Inc.
Other product and company names (or logos) mentioned herein may be the trademarks of their respective owners.
<http://www.metaintegration.com>

3. Release Changes

OMM 12.2.1.3.0 based on MIMM OEM 10.0.0 (09/21/2018)

• BRAND NEW USER INTERFACE EXPERIENCE

◦ METADATA MANAGER VS METADATA EXPLORER UI:

- In previous OMM versions, the OMM Web Application Server has offered two different User Interfaces (UI) targeting different user communities. The original Metadata Manager UI was designed for the advanced technical users with a traditional development tool layout including multiple panels: tree structure on the left, multi-tab windows in the middle, attributes on the right, and log activities at the bottom. The Metadata Manager UI also presents the highest level of details and complexity of all harvested metadata. The Metadata Explorer UI was initially introduced as a read only UI with simpler metadata for business users offering an easy to use layout for multiple devices, including tablets. The Metadata Explorer became the new UI platform for all new editing capabilities such as the business glossary or data modeling.
- With OMM v12.2.1.3, all other editing capabilities are now available in the Metadata Explorer UI, including data mapping, enterprise data architectures (Configuration editor and model stitching), and even the Administration features like Custom Attributes which are now under are now available in the Metadata Explorer UI > Manage > Custom Attributes. Consequently, the Metadata Manager UI is now only necessary (and therefore available) in the OMM Advanced Editions for repository management (with multi version and configuration management). The OMM Standard Edition v12.2.1.3 is now fully implemented in the Metadata Explorer UI where Manage > Content allows users to directly create models to the default single configuration, import metadata, stitch models (connections), and trace lineage right away.

◦ METADATA HOME PAGES:

New metadata home pages with multiple top tabs offer quick access to all key information:

- The first tab is always the Overview tab which provides a dashboard to all critical information and properties.
- The next set of tabs are specific (metamodel / profile driven) to the type of object, for example:
 - Database Table objects have tabs for Columns and Constraints.
 - BI Reports (like Tableau Workbook) objects have tabs for Dashboards, Worksheets, and Data sources.
- The next set of tabs are for the common critical metadata analysis:
 - DATA FLOW for data lineage and impact analysis.
 - RELATIONSHIPS for detection, management, and curation of relationships (see new features below)
 - SEMANTIC FLOW for definition and usage perspectives (see new features below)
- The last set of tabs are for common documentation and administration like: Comments, Attachments and Audit Log.

- METADATA QUICK ACCESS:

Much improved ways to quickly access the right metadata:

- SEARCH has been massively improved in both real time performance (now based on Lucene) and in functionality as a metadata driven search with natural language semantic search (see new features below)
- BROWSE has also been massively improved in both performance (now also Lucene based) and in functionalities as a metadata asset type driven browser with support for hierarchical display at all levels of any data sources including database, DI, BI, Data Lakes, and even No SQL (like JSON hierarchical structures)
- Enterprise ARCHITECTURE driven graphical navigation allows users to drill down from a top down big picture of the enterprise architecture.

- METADATA REPORTING:

Brand new powerful unified metadata reporting capabilities where both search and browse end up to the same reporting page which is also directly available at Browse > Report. Starting from search simply predefines the text filtering (e.g. customer), while browsing predefines a category (e.g. database / tables), and direct access to reporting does not predefine anything.

- The reporting capabilities offers to select multiple categories (e.g. database / tables + Flat files) and subset by content (My Data lake + Sales DW database) before drilling down with the following filters:
- Then filtering is available for Last Modified, Stewards, Labels, Semantic Types, Endorsed By, Certified By, Created By, Warning By, and Commented By.
- Finally, more custom filtering per attribute (including custom attributes) common to the metadata subset (e.g. SecurityLevel = Orange).
- Reports can be reused by saving the URL as favorites (further versions will support full report management within the application)

- METADATA USER LISTS:

Brand new user list management feature allows users to define and manage lists of metadata objects. Just like labels, lists are available anywhere in the UI to add/remove objects, bulk editing, and management. Lists can contain any type of metadata such my favorite list of terms, tables, or reports. Lists can also contain multiple type of content such as my to do list with terms, tables, and reports in that list. Lists can be shared with other users when marked as public, such as our quarterly review list. Note that lists are flat, therefore not hierarchical and with no sub-list or include concepts.

- METADATA TAGGING WITH LABELS:

The metadata tagging with labels has been much improved to be harmonized with the brand-new list management experience in order to facilitate adding/removing objects anywhere, grid editing, and more.

- METADATA DOCUMENTATION:

Much improved ways to document metadata:

- MULTI-LINE TEXT has been introduced (in addition to the previous single line Text for better formatting and layout. In addition, Multi-Line text has been enhanced with support for URL links and embedded image attachments using a JIRA like syntax. Multi-Line Text is not only the default format for all Descriptions and Comments, but is now also available as a new type of Custom Attribute that can be applied to any metadata for documentation.
- RICH TEXT Documentation with (WYSIWYG) Visual Edition is not only the default medium for Glossary Term documentation, but is now also available as a new type of Custom Attribute that can be applied to any metadata for documentation.
- SQL TEXT of SQL View, Stored Procedures and more are now better presented with colored syntax and optional reformatting. Note that this is not a new type of custom attribute but any predefined attribute with SQL is better formatted.
- ATTACHMENTS (such as pictures, documents, etc.) have been enhanced as part of its integration with the new Metadata Explorer, including Management (Drag and Drop), Preview, and Thumbnails that can be embedded in the Text (and Multi-Line text) descriptions, comments and custom attributes.

- DATA CATALOGING

- Brand new Data Cataloging applications well integrated with the existing Data Governance (DG) capabilities, and based upon the solid Metadata Management (MM) foundations with full data lineage and powerful metadata version and configuration management.
- Managing both modern cloud based data lakes and classic Data Warehouse (DW) Enterprise Architectures
- Harvesting metadata from both modern (XML, JSON, Avro, Parquet, ORC) files, Hive tables, and Kafka messages), and classic (relational tables / CSV files) data technologies

- DATA MODELING AND DOCUMENTING ANY HARVESTED METADATA

- In OMM v12.2.1.2, existing data stores such as RDBMS could be harvested as a Physical Data Model (PDM) instead of a simple Model, in order to offer full documentation including business glossary term reuse based upon automatic semantic links, reverse engineering based upon naming standards, data modeling with diagramming, and of course automatic change management (re-harvest/compare/merge).
- In OMM v12.2.1.3, all the above capabilities are now available on any harvestable model content without having to create a PDM. In other words, any data integration, business intelligence, reports, data stores (relational, hierarchical, NoSQL, files, etc.) can be documented at as needed, including support for relational data models. Consequently, all existing PDM in OMM v12.2.1.2 may be converted to Models in OMM v12.2.1.3 without loss of any existing documentation (including diagrams).
- The documentation (business names and definitions) process has been improved allowing any object (e.g. table, column, report field) to be quickly and easily:
 - "Classified" with a local semantic link to a glossary term, without having to use an intermediate Semantic Mapping content, or associating the Model to a Glossary as with the PDM.
 - "Documented" with a local business name and definition overwriting any Semantic link (Classified, Mapped or Inferred)

Furthermore, this documentation process is also dramatically enhanced through the integration with a new "Semantic Flow" tab acting as an interactive dashboard on finding the right definitions (see below).

- When harvested databases that are already documented in data modeling tools (e.g. Erwin), such data models can be imported as a separate model and automatically stitched directly to its matching harvested database (without using any semantic mapping model). The semantic stitching is automatically maintained as both the database and its associated data model are independently re-imported/refreshed on regular basis (the stitching will report inconsistencies). From the user perspective, the documentation (business name, descriptions, relationships, diagrams) of any harvested database table / column is automatically inherited from its associated data model.
- RELATIONSHIPS Discovery & Management
 - Relationship Discovery using the following methods:
 - Automatically "Inferred" based on:
 - Metadata Usage Driven: using the surrounding data flow usage such as joins in DI (ETL Tools, SQL Scripts or Data Prep) and BI (traditional or self-service) activities.
 - On Demand "Detected" based on:
 - Metadata Name Matching: for example PurchaseOrder.SKU = Product.SKU or Customer.AccountId = Account.Id
 - Semantic Definition Matching: classified by users to the same glossary term.
 - Relationship Management with user defined relationships and social curation (e.g. endorsed or certified joins)
 - Dynamic Data Model diagram generation from Relationships surrounding any object (e.g. table or file).
- SOCIAL CURATION
 - Endorsement, warnings, certifications with impact on search ranking.
- SEMANTIC SEARCH
 - Metadata driven search language such as "Customer tables" for any tables with Customer in the name, "tables with SSN" for any table with a SSN column (e.g. for GDPR), or "ROI in Reports" for any reports containing ROI.
- SEMANTIC MAPPING
 - Major improvements in semantic mapping including in place semantic mapping via two approaches:
 - Top-down from Business Glossary Term or Data Model Entity/Attribute,
 - Bottom-up from Data Store Tables/Columns or Report Fields.
- SEMANTIC FLOW
 - Major improvements on the semantic flow analysis now also supporting the documentation process acting as an interactive dashboard for finding definitions that are:
 - "Local" (within the Model) that has been either "Imported" (metadata harvesting) or locally "Documented" (edited description overwrite),
 - locally "Classified" (within the Model) to an external glossary term,
 - directly "Mapped" via a Semantic Mapping Model or direct stitching (e.g. between a database and its data model),
 - indirectly "Inferred" through complex data flow pass through and semantic flow (which can be graphically analyzed in the data flow diagram), or
 - "Searched" for by name in all glossaries.
- Any of the Searched, Inferred or Mapped definitions may quickly (in place) be reused/promoted as a Classified or Mapped definition.
- RELATED REPORTS
 - Related Reports are now available on any metadata objects such as files, tables, columns, etc. (instead of just business terms). This allows business users looking at the result of a search to have direct access to a simple list of any related reports in any BI tools (crossing all semantic and data flows without exposing any of the complexity to business users) Such reports can then automatically be opened in their respective BI tool technologies, therefore acting as a multi-vendor BI tool web portal for business users.
- DATA CONNECTIONS / METADATA STITCHING
 - Complete support for file format harvesting and stitching.
 - Connection pool factorization (e.g. from DI and BI servers) to minimize the number and complexity of stitching connections.
- DATA MAPPING Specifications & Design
 - The Data Mapping Specifications and the Data Mapping Designs have been fully resigned and merged into brand new Data Mappings that can be used for multiple purposes, including capturing data flow mapping requirements.
 - The Data Mapping tool allows for the mapping of multiple source data stores into a target data store in multiple steps with (schema or table level) Bulk Mappings and (column/field level) Query Mappings. The data mapping tool offers new graphical mapping visualization as you map, and new expression syntactical editors when designing joins, lookups, filters, etc.
- ARCHITECTURE, DEPLOYMENT & INTEGRATION
 - Search engine re-designed and optimized with Apache Lucene offering near real time metadata search and navigation (and removing any dependencies of underlying database text search requirements)
 - Third party software upgraded to the latest of Java 8, Apache Tomcat 9, and more for security and performance improvements.
 - Single Sign On (SSO) integration architecture has been redesigned for easy external authentication with redirect using custom scripts in any language such as Python (Note that OMM v12.2.1.2 external authentication required custom complex integrated java scripts). Post GA cumulative patches will

include support for the Security Assertion Markup Language (SAML) standard, and native cloud authentications such as Amazon AWS and Microsoft Azure.

- UPGRADE REQUIREMENTS:

- CPU & MEMORY:

The OMM v12.2.1.3 now uses Lucene as the search engine instead of using the text search capabilities. Consequently, the overall hardware requirements now demand as much processing resources (CPU and memory) on the OMM Application Server machine as on the underlying Database Server machine. (OMM v12.2.1.2 used to demand more resources on the database server as all searches were performed using the database server).

- UPGRADE PROCESS:

- OMM v12.2.1.2 SOFTWARE UPGRADE & DATABASE MAINTENANCE:

You must download and apply the latest OMM v12.2.1.2 Cumulative patch (July 2018 or newer), and make sure the OMM v12.2.1.2 software still works properly after that step.

You must then make sure that the regularly scheduled database scheduled has run successfully and long enough to have no further actions to do (such as purging deleted content from the database)

- OMM v12.2.1.2 DATABASE BACKUP:

You must then perform a full database backup (OMM, data, indexes and scripts), restore it on a brand new (different) database server, and make sure the OMM v12.2.1.2 server software still works properly after that step.

(Do not rely on the OMM backup script for that process, you must use real full database backup).

- OMM v12.2.1.3 SOFTWARE INSTALL & DATABASE UPGRADE:

Install the OMM v12.2.1.3 software on a new directory (independently of the OMM v12.2.1.2 install directory). Use the Setup utility to point to the database to upgrade. Starting the new OMM v12.2.1.3 server will automatically perform an upgrade of the database's OMM data and scripts. Note that OMM v12.2.1.3 uses Lucene on the OMM server for search, therefore the database will no longer need to use text search indexes and will therefore need less space in the database

- POST UPGRADE:

- FLAT FILES:

OMM v12.2.1.2 had no proper support for flat files which are now fully supported as part of the new data cataloging capabilities of OMM v12.2.1.3. Therefore, the early Flat File (CSV or XLSX) prototypes beta bridges have been discontinued and replaced by the import bridge from File System (CSV, Excel, XML, JSON, Avro, Parquet, ORC), or the other new file system / object store import bridges such Amazon S3, Azure Blob Storage, Hadoop HDFS, etc. which can all contain flat files. All these file system import bridges now create multi-model content which can be stitched to data mappings and other DI/ETL models. Any content imported from Flat File (CSV or XLSX) prototypes beta bridges can still be visible in OMM v12.2.1.3, but no further imports can be performed, and migration to the new bridges cannot be automated (different parameters and different content type from single to multi model). Therefore, new models should be created with the new file system bridges, and the old content (from the prototype beta bridges) should be deleted.

- PHYSICAL DATA MODELS (PDM):

In OMM v12.2.1.2, PDM were used to document (including data model diagrams) existing databases, as well as designing new databases (new tables, columns, etc.). In OMM v12.2.1.3, PDM is no longer needed to document existing databases (including data model diagrams, glossary integration, etc.). Consequently, OMM servers can no longer create new PDM models, although any existing PDM created with OMM v12.2.1.2 are still operational on OMM v12.2.1.3. The bottom line is that the OMM v12.2.1.3 new way to document data stores / databases is not only as powerful as PDM but it is much more efficient with version management (changes after new harvesting). Consequently, we recommend all PDM models used to document databases to be converted to models which can be performed without any loss of documentation, by means of a conversion script available on PDM models.

OMM 12.2.1.2.0 based on MIMM OEM 9.1.0 (06/30/2017)

- HARVESTED MODEL CHANGE DETECTION avoids systematically creating a new version of the content upon scheduled harvesting of large database, data modeling, data integration, or business intelligence servers. This is automatically performed as side effect of any new harvesting by a systematic and efficient (fast) model comparison with the previously harvested metadata. This dramatically reduces the needed database space by creating fewer versions, and enable the possibility of reliable notification only if a change really occurred. Note that in previous versions, the incremental harvesting already offered systematic and automatic reuse of unchanged models (e.g. BI Reports) from a large a multi-model server (e.g. BI server)
- SUBSCRIPTION / NOTIFICATION mechanism on select changes at both the repository model level (e.g. a new version of a data store is harvested) and at the model object level (e.g. a terms changed or ready to approve/review in a Business Glossary under Workflow). Anyone may be assigned stewardship roles and thus will be notified as new imported content is harvested, with links back to the new object and the ability to compare using the newly re-written powerful comparator, and the ability to identify impacts of change for any architecture or configuration of assets.
- CUSTOM ATTRIBUTES on any harvested metadata (models) from data stores, data modeling, data integration, and business intelligence tools. Therefore allowing to tag any metadata (from Hive tables to BI reports down at the column/field level) for custom properties such as a company confidential level that can be read for external products on security enforcement and compliance. Note that in previous versions, these same custom attributes could already be applied to authored metadata (models) such as terms of Business Glossaries or tables/columns of Data Models.
- BUSINESS GLOSSARY WORKFLOW for the business users behind the Metadata Explorer UI. Note that in previous versions, a (customizable) Workflow was already available in the Metadata Manager.
- DATA INTEGRATION BROWSING AND LINEAGE for the business users behind the Metadata Explorer UI, allowing them to browse the data integration jobs (from DI/ETL/ELT tools as well as SQL Scripts) and analyze the summary data flow lineage of their execution. Note that in previous versions, the browsing (open) and full detailed data flow lineage of any data integration models (DI/ETL/ELT and SQL scripts jobs) were already available in the Metadata Manager (and still are).
- DATA CONNECTION STITCHING MAJOR IMPROVEMENTS now offering to stitch by column position (needed in SQL insert statements of ETL scripts), and smart case aware stitching (as some database's name spaces like schema/table/column are case sensitive while others are not)
- BULK DATA MAPPING at the table level.
- MODEL COMPARE/MERGE: The comparison facility has been completely re-written to include comparison for every level of detail for those models with the same profile (e.g., data model from one technology and data model from another). Even entirely different contents (e.g., an ETL and a data model, or a BI Design and Glossary) may be compared, only at a lesser level of granularity (basically at the granularity of stitching, e.g., schema, table, column). Finally, for physical data models (including documentable models based upon harvested database structures) one may use a powerful merge feature again with full control down to any level of granularity.

- DATA MODELING Major improvements and new features involving the physical data modeling capabilities centered around a data documentation tool enabled through physical data modeling based upon the structure harvested from existing data stores of the data warehouse and data lake (including traditional RDBMS and Hadoop Hive big data) Also includes new advanced support for physical data model diagram editing, relationships definition, all the way to export to data modeling tools, business intelligence design, etc., and comparison/compliance with live database / big data hive implementations..
- REST API SDK major enhancements with many new features
- LIGHTWEIGHT MODELS: Model content (such as a harvested databases or data models) can be stored in the repository as a lightweight model (just the XML file), or fully expanded (as both XML file and fine grained repository objects). When retaining many historical versions of a model, using lightweight models saves repository space, and also avoids slowing down the search by not indexing historical repository objects. Lightweight models cannot be directly used in a Configuration or in a Mapping. However, the lightweight model of a data store (such as a RDBMS or Hadoop Hive) can be documented with a Physical Data Model (PDM) for data model diagramming and semantic linking to a Business Glossary (BG). Such a PDM can of course be used in any Mapping or Configuration to be exposed to business users in the Metadata Explorer. Note that lightweight models can immediately (without any loss of performance) be opened in the Metadata Manager (to browse metadata or trace lineage within that model), Compared (with the Model Comparator to analyze the difference between versions), Exported (for example to BI design tool).
- UPGRADE NOTES: The Business Glossary Workflow has been significantly improved in the metadata explorer. Therefore, before upgrading to this version, it is strongly recommended that all business glossaries under workflow have published terms only (this can be achieved by listing all draft terms and either publishing or reverting them to the previously published state). Otherwise, the upgrade process will systematically publish all draft terms in their current state (which can be undesirable if the current state is not what you would like to publish). Finally, after the upgrade, you will need to manually re-enable the Workflow on these Business Glossaries.

OMM 12.2.1.1 based on MIMM OEM 9.0.2 (06/10/2016)

- METADATA MANAGER:
 - Major improvements in MODEL VERSION / CHANGE MANAGEMENT preventing the creation of unnecessary new versions of models if the source metadata (e.g. a database, or data model) has not changed since the last automatically scheduled metadata harvesting. This is new feature is achieved by taking advantage of the MIMB's new capabilities to compare the metadata of a newly imported model with a previously imported one in order to detect any change. The major benefit of this new feature is to dramatically reduce the disk space in the repository by automatically deleting unnecessary versions.
 - New CONFIGURATION / VERSION CHANGE MANAGEMENT capabilities offering a comparator of versions of configurations.
- METADATA EXPLORER:
 - Major redesign of the Metadata Explorer UI on both the look & feel and actual capabilities.
 - New METADATA SEARCH/BROWSE with FILTERING AND REPORTING capabilities offering:
 - New Search (or Browse) with Filtering capabilities on any attributes/properties
 - New choice of result display as a classic Google like "LIST", or a new powerful "GRID" offering a spreadsheet like display of multiple attributes/properties at once. Such attributes/properties can be individually selected, reordered, and sorted, basically offering a full metadata reporting solution. The results can of course be downloaded as CSV/Excel files.
 - New METADATA EDITING Capabilities at many levels including:
 - Numerous new fast and easy "in place" editing to Rename objects, Edit Descriptions, and more.
 - The new Search/Browse GRID display also offers efficient editing with:
 - TABULAR EDITING of multiple objects at once such as Business Glossary Terms, Data Models Tables, or Table Columns
 - BULK CHANGE of multiple objects at once, where a search can return multiple objects (that can then be selectively subsetted) for which changes can be performed at once (e.g. Change the Security Threat Level to Orange to a set of tables at once)
- METADATA AUTHORIZING TOOLS:
 - Common Features:
 - Major improvements in CUSTOM ATTRIBUTES (also known as User Defined Properties) to objects of the Business Glossaries and Data Models
 - Custom Attributes are now common to the OMM repository (e.g. Security Threat Level = [Red, Orange, Yellow, Blue, Green] and are therefore shared between Business Glossaries, Physical Data Models, etc. Therefore, having a centralized place for maintenance (e.g. adding a new value: purple)
 - Custom Attributes can now have a default value (e.g. default value is green)
 - Custom Attributes now have a much wider scope to be applied at any level from a high level repository object (e.g. harvested Model, Data Mapping, Directory) to fine grain model objects (e.g. A Business Glossary / Term, and/or a Physical Data Model / Column)
 - Custom Attributes now have a security group associated to them (e.g. the Security Threat Level custom attribute may only be set by a custom Security Approved group)
 - New AUDIT TRAIL for any changes in objects of Business Glossaries and Data Models, including who changed a given attribute and when
 - BUSINESS GLOSSARY:
 - New Business Glossary editing capabilities are now available to the business users under the Metadata Explorer UI. (includes tablet friendly in place editing, as well as HTML formatting of descriptions, etc.)
 - DATA MODELING:
 - PHYSICAL DATA MODEL (data documenter for existing data stores databases, data warehouse, data lake):
 - NEW feature with this version of OMM
 - DATA MAPPING:
 - DATA MAPPING SPECIFICATIONS (Data Flow Mapper)

- Minor improvements and bug fixes

- ARCHITECTURE & TECHNOLOGY:

- Major database performance improvements
- Updated OMM Web Services which are now based on RESTful API technology (i.e. therefore removing any security vulnerabilities of the older Axis technology)

OMM 12.2.1.0 based on MIMM OEM 9.0.1 (12/15/2015)

- ARCHITECTURE & TECHNOLOGY:

- 100% Java delivery and installation allowing support for Windows as well as a variation Linux/Unix deployments
 - The Metadata Management Server (OMM) can now be installed on Unix/Linux variations.
 - The Metadata Harvesting Agent (MIMB bridges) can be installed:
 - Locally (co-located with a OMM server on Linux) to run 100% java based bridges including JDBC database bridges (Oracle, Teradata, DB2, SQL Server, etc.), big data bridges (Hadoop Hive, HCatalog), and other popular bridges such as CA ERwin xml, Informatica PowerCenter xml, Tableau BI, etc.
 - Remotely on a Windows machine for C++ based bridges and COM API based bridges requiring software SDK running on Windows such as CA ERwin native (.erwin) files, and many BI tools like SAP BO Universe, Microstrategy, QlikView, etc.
- 100% HTML 5 (no more Flash) and tablet friendly look & feel, allowing to run on Mac, Tablets, and more
- Metadata Explorer Customization to offer a better experience to targeted business users of the customer company:
 - Customize headers, company logos, menus, search categories, home page (with search widgets), automatic opening of reports (BI portal experience, BI report documentation (adding BG terms)
- Improved Metadata Explorer Search Performance
- Improved Data Integration (DI/ETL/ELT Import Bridge) Harvesting Performance
 - Now offering detailed DI data flow lineage analysis on demand only (in real time), instead of pre-calculating even if unused

OMM 12.1.3.0.2 based on MIMM OEM 8.0.3 (05/19/2015)

- DATA MODEL DIAGRAM VISUALIZER:

- Major improvements with the HTML5 redesign including better scalability, performance and overall layout quality
- New interactive search
- New diagram auto layout
- New dynamic layout of a diagram subset starting from an entity with all related entities with one or two levels of relationships (very useful for large diagrams)

- SEMANTIC MAPPER:

- New support for BI Report metadata (such as a page of a workbook, a table or pie chart on page, or just the axis of a graph), allowing to document precise items within a given report by associating (semantic links) business glossary terms to them.
- New support for models within a multi-model server source, allowing to provide documentation (or glossary) at the high level of a given data model (or BI report) within a multi model server, such as:
 - a Data Modeling (DM) repository server with many data models inside (e.g. CA ERwin Mart)
 - a Business Intelligence (BI) content server with many BI designs and BI reports inside (e.g. SAP BusinessObjects)

- BUSINESS GLOSSARY:

- New customizable role driven workflow support (can be turned off) and security enforcement

- METADATA EXPLORER UI:

- New integrated presentation of Business Glossary terms related to any data store or BI report objects, including the ability to add/remove BG terms documenting a data store or BI report
- Improved search support for auto complete and objects

- ADMINISTRATION:

- New group based security model (as side effect of the new role based Business Glossary workflow)

- ARCHITECTURE & TECHNOLOGY:

- New support for HTML5 only devices like iPad and other tablets (Flash will no longer be needed) for graphically tracing any data flow or semantic lineage (Lineage Analyzer), and for visualizing data models (Diagram Visualizer).
- Java 8 (compiled with backward compatibility with Java 7) compliance (Java 6 is no longer supported)

OMM 12.1.3.0.1 based on MIMM OEM 8.0.1 (12/02/2014)

- FEATURES:

- New "Show Related Reports" (e.g. from a Glossary Term)

- METADATA MANAGER UI:

- New Metadata Manager look & feel (to match the Metadata Explorer)
- New Business Glossary batch editing
- METADATA EXPLORER UI:
 - New customizable action menus per repository object type (e.g. open BI report with BI tool by default)
 - New dedicated web pages for tracing data lineage & impact, and semantic definition & usage
 - New access to the Configuration's Enterprise Architecture Diagram

OMM 12.1.3.0.0 based on MIMM OEM 8.0.0 (10/01/2014)

- Initial Release

4. System requirements

4.1 Important preliminary disclaimer notice on all requirements

The following requirements only define the minimal requirements to run the application server with reasonable performance based on the provided tutorial, or small business use cases. The actual requirements for enterprise wide use cases based on larger models and configurations do require significantly greater resources to obtain acceptable performance.

The following requirements are based on:

- actual physical hardware (no virtual environment),
- minimal to no network overhead (assuming both the database and Application servers to be locally installed),
- vendor's default install of the current version of their software (with all current service or fix packs),
- no other applications sharing such hardware (starting from a clean machine),

Any other hardware/software configurations are acceptable as long as they provide the same (or better) results on the provided performance benchmark. In such case, if any problem is discovered (e.g. scalability or performance issues), then the customer must be able to reproduce the issue using an environment that conforms to the minimum performance requirements as defined herein.

Potential known issues include (but are not limited to) the following:

- actual usable hardware performance on virtual environments (e.g VMWare configuration and licenses)
- network overhead on remote servers (e.g. bandwidth, proxy, VPN issues, VMWare inter OS network limitations without a proper license, etc.)
- shared resources with competing applications on the same OS, or between OS on a virtual environment,
- licensing limitations (e.g. most database server licenses limit the number of usable core/CPU)
- vendor software known limitations and requirements (e.g. Oracle on VMWare vs Oracle VM)

4.2 Web Client requirements

Users only need an internet browser:

- [Google Chrome](#) v67 or newer
- [Microsoft Internet Explorer \(IE\)](#) v11 or newer, and make sure it is NOT working in IE 10 compatibility mode (Settings > Compatibility View Settings: no checked boxes).
- [Microsoft Edge](#) v41 or newer
- [Mozilla Firefox](#) v61 or newer
- [Apple Safari](#) 11.1 or newer

4.3 Application Server Requirements

Hardware Minimum Requirements (based on physical hardware performance, not a virtual environment):

- 2 GHZ or higher quad core processor
- 8 GB RAM
- 10 GB of disk space (all storage is primarily in the database server)

Operating System Requirements:

- Microsoft supported Windows 64 bit versions (including Windows 2008 Server, Windows 2012 Server, Windows 7, Windows 8.x, and Windows 10).
 - Ensure that installer is executed with full Administrator privilege
 - Ensure that Microsoft .NET Framework 3.5 or higher is installed
 - Ensure that all current Microsoft Windows critical updates have been applied
- Most popular Linux/Unix 64 bit Operation System Versions (such as Oracle Solaris, Redhat or Mac OS).
 - This software is not based on code compiled for any particular Operation System OS (e.g any particular Linux distribution or version), therefore, the supported OS are 100% based on the supported OS of the underlying Java Runtime Environment (JRE) and Tomcat software (see their supported platforms for further details).

Application Server Engine Requirements:

- Apache Tomcat 9 - 64 bit (bundled)
- Other Application Servers (such as IBM WebSphere or Oracle WebLogic) require manual install/setup, and are therefore not supported by this version.

Java Runtime Environment (JRE):

- Oracle JRE 8 - 64 bit (bundled and recommended)
- Other Java Runtime Environment (JRE) (such as IBM Java) require manual install/setup, and are therefore not supported by this version.

4.4 Database Server Requirements

Hardware Minimum Requirements (based on physical hardware performance, not a virtual environment):

- 2 GHZ or higher quad core processor
- 8 GB RAM
- 20 GB of disk space (or more as needed for the data)

The OMM Database Server can reuse your existing Oracle database server:

- **Oracle 10g R2 to 12c - 64 bit** (recommended for large enterprise, default supported version)
 - The character set of the database must be AL32UTF8 (UTF8).
 - In order to find out what exact Oracle edition/version is actually installed:


```
sqlplus.exe SYS@<DB-NAME> as SYSDBA
          select banner from v$version where BANNER like '%Edition%';
```
 - In order to find out how much memory is actually available to the Oracle database, it is important to first understand [how Oracle's memory is configuration and used](#):
 - The actual available [System Global Area \(SGA\)](#) memory can be found using:


```
sqlplus.exe SYS@<DB-NAME> as SYSDBA
              show sga;
              select * from v$sga;
              select * from v$sgainfo;
```
 - The actual available [Program Global Area \(PGA\)](#) memory can be found using:


```
sqlplus.exe SYS@<DB-NAME> as SYSDBA
              select * from v$pgastat;
```
 - In order to find out how much processing CPU/Cores is actually available to the Oracle database, query the table [v\\$parameter](#) for the value of [cpu_count](#), or query the table [v\\$license](#) as follows:


```
sqlplus.exe SYS@<DB-NAME> as SYSDBA
          select * from v$license;
```

Database Administrator privileges are required to install/setup/uninstall the database.

In general, one must ALWAYS install the latest service packs for a given database version BEFORE creating the OMM database. E.g., for Oracle 11.2 one is required to apply the patches to upgrade to 11.2.0.3, or whatever is the latest patch level at the time. In addition, Oracle 11.2.0.4 must have patch 17501296 applied.

Virtual Memory: For a Windows based database server, be sure to either:

- set the page file size to be managed automatically by OS
- or it should be at least 3 times the memory or RAM size for the machine.

Thus, you must have more than that much free disk space (at least 3 time the amount of memory or RAM) on the drive where the page file is defined to reside.

5. Database Server Setup

The OMM Application Server requires the connection to an existing Database server for metadata storage (metadata repository)

The following database setup scripts and instructions assume the following by default:

```
Database Name: MM
Database User: MM
Database Password: = MM123! The database name and user name can be changed, and the password should of course be different.
```

After the product is fully installed and web connectivity has been made, one may connect to a different database by way of the web based user interface at Tools -> Administration -> Database.

5.1 Database on Oracle

Create a user MM and a database MM with the following privileges:

```
sqlplus.exe SYS@<DB-NAME> as SYSDBA
```

```
-- Delete previous user and database if needed
-- DROP USER MM CASCADE;

CREATE USER MM IDENTIFIED BY MM123!;

GRANT CONNECT TO MM;

GRANT CREATE TABLE TO MM;
```

```

GRANT CREATE VIEW TO MM;
GRANT CREATE SEQUENCE TO MM;
GRANT CREATE TRIGGER TO MM;
GRANT CREATE PROCEDURE TO MM;
GRANT CREATE TYPE TO MM;

GRANT EXECUTE ON DBMS_LOB TO MM;

-- If you get the error "Database exception occurred: ORA-01950: no privileges on tablespace 'USERS'"
-- ALTER USER MM QUOTA UNLIMITED ON USERS;

```

6. Application Server Setup

6.1 Application Server Installation and Configuration

The OMM Application Server is installed as follows:

- On **Windows** operating systems, use `unzip` to extract the software package (.zip) in the directory of your choice. You should avoid using the "Program Files" directories of Windows 7, 8.x and 10 as they have are now controlled by Windows with special access rights. Depending, on your software installation directory, you may need "Administrator" privileges.
- On **Linux** operating systems, use `tar -xjvf` to extract the software package (.tbz2) in the directory of your choice. Depending, on your software installation directory, you may need "root" privileges.

If you are using an existing database and do not wish to customize the application server (e.g. memory allocation, Windows services), then you can skip this step and go directly to the section on [Application Server Execution and Initialization](#)

Otherwise, go to the software home directory and "run As Administrator" the **Setup** utility (.bat on Windows or .sh on Linux). This setup utility will allow you to setup the configuration parameters defined below through a user friendly application. After any change on any panel (tab) below, remember to press the **Configure** button in order to perform the configuration changes. A dialog box will be issued to confirm success or failure (with error messages). Alternatively, this setup utility also works at the Windows command line or Linux shell, use the `-help` options.

- Product Edition** tab:
 - Oracle Enterprise Metadata Management (OEMM)**
 - Oracle Metadata Management for Oracle Business Intelligence (OMM4OBI)**
- Application Server** tab:
 - Enable Windows Service**
This will create the "OMM Application Server" Windows Service, set it for automatic start, and actually start it. Unchecking that box will delete the "OMM Application Server" Windows Service, which is a good idea before uninstalling the OMM software.
 - Metadata Harvesting Server Only**
This allows to setup this application server as a metadata harvesting server only, rather than a full metadata management server. This is very useful in architecture deployments where the metadata management server is:
 - deployed remotely on the cloud but needs to access metadata harvesting servers (agents) locally on premise, or
 - deployed on Linux but needs to access metadata harvesting servers (agents) on a Windows machine where DM/DI/BI client tools are Windows only (e.g. COM based SDK).
 - Metadata Harvesting Browse Path**
This controls the access to the file system for metadata harvesting. The default value is set to "*" which means any Windows drive (C: and any mounted remote drive R:) or any directory from root on Linux. It is strongly recommended to limit the access to a common shared data location, and avoid system area.
 - Data Directory**
This is the location of all data files, including log files as well as the metadata harvesting caching. The data directory is located by default in the 'data' subdirectory of the application server home directory. It is recommended to separate the program data from the program files, this allows you to provide a new location for the data in a separate area (with regular backups if possible). Note that changing to a new location will not move the existing data from the previous location. Either the new location already had the data (from a previous install), or new data will be created.
 - Max Memory**
This defines the maximum memory used by Java (JRE) on the OMM Application Server (Apache Tomcat). This is unrelated to the maximum memory used by Java on bridges for Metadata Harvesting which is separately set by default with the `M_JAVA_OPTIONS` variable in `%OMM_HOME%\conf\conf.properties`, and can be overridden within the Miscellaneous parameter of memory intensive import bridges (e.g. JDBC).
 - Port Number**
This sets a custom start port number by default to avoid conflicts with other web application servers. Note that the OMM Application Server uses 2 consecutive ports. However, this can be set back to 80 to avoid having to specify any port number in the URL.
 - SSL**
This enables Secure Socket Layer (SSL) communication for web access (HTTPS). In order to support HTTPS, the OMM Tomcat service must be configured to work with HTTPS for encryption of passwords and other content exchanged between the web client and the OMM Application Server. In this case, you will need a certificate for the HTTPS protocol to work. Note: the OMM software does not perform any error handling for validating a certificate associated with the OMM Application Server, and most web browsers will report an error if the certificate is not provided by a valid certificate authority. Thus, your certificate should be a trusted certificate provided to you by a valid Certificate Authority.
 - Certificate file**
Mandatory - Can be a .pem (privacy enhanced electronic mail), .pfx (Windows personal information exchange) or a .jks (Java keystore)

- **Root Certificate file**
Optional (only required if the above certificate file was generated by an external company as a certificate authority)
- **Key file**
Optional (often it is the case that the certificate file also contains the key)
- **SSL Key Password**
Optional (required if the key is password protected)

6.2 Application Server Upgrade

6.2.1 Understanding the Data Locations

Most application data is obviously located and your database server, you are responsible for regular backup of such database. Upgrading your application will also upgrade the associated database content (database schema, stored procedures, indexes and of course data). Therefore make sure you always backup your database before any upgrade.

Furthermore, the upgrade process may take several hours (on large repositories) and also need extra space for temp data during the migration. Therefore make sure the database has at least 20% free space.

However, it is also important to understand that the software installation directory (known as `%OMM_HOME%` in this document) also contains some critical application data and application setup customizations that have to be taken into account in your backup or upgrade process, including:

- `%OMM_HOME%\data`
which contains other application data such has the metadata harvesting cache (critical for incremental harvesting, and metadata export), the application server cache (Tomcat), the log files (metadata harvesting with MIMB and Tomcat), and other temp files. Remember that the actual location of this OMM Application Server data directory can be configured with the Setup utility (in the "Application Server" tab).
- `%OMM_HOME%\conf`
with the `conf.properties` file containing most customizations defined with the Setup utility (in the "Application Server" tab), and the `\resources` directory containing any [User Interface Customizations](#).
- `%OMM_HOME%\tomcat\conf`
with the `tomcat.properties` file containing the tomcat port and memory customizations defined the Setup utility in the "Application Server" tab, and the `keystore` file containing the tomcat SSL certificates defined with the Setup utility (in the "Application Server" tab).
- `%OMM_HOME%\jre\lib\security`
which also contains some SSL customizations defined with the Setup utility (in the "Application Server" tab). It is recommended to not reuse such directory, but rather reinstall the SSL keys with the Setup utility.

6.2.2 Upgrade Process

We recommend the following upgrade process:

- Stop the OMM Application Server (possibly using the Windows services).
- Backup your previous installation by renaming the `%OMM_HOME%` directory as `%OMM_HOME%.old` and then install the new software package at the exact same previous location: `%OMM_HOME%`
- Restore your data and customization/setup by copying the appropriate files and directories (as previously explained) from `%OMM_HOME%.old` to `%OMM_HOME%`, including at least `\data` and `\conf\conf.properties` but possibly more as used and customized such as `\conf\resources`, or `\tomcat\conf`.
- Finally, restart the MIMM Application Server (possibly using the Windows services) which may prompt you for a database upgrade of the MIMM tables.

Finally, remember that any upgrade may also bring many new and improved import bridges that may harvest extra metadata. Therefore, any upgrade must also be followed by a re-harvest (import) of Models, and re-build of Configurations to take advantage of the new capabilities.

6.2.3 Version Specific Upgrade Issues and Recommendations

Upgrading to a new version may have version specific issues or recommendations that are listed at the bottom of the release notes: see [Release Changes](#) for more details.

6.3 Application Server Execution and Initialization

The easiest way to start the OMM Application Server is to go to the software home directory and use the `RestartApplicationServer` utility (.bat on Windows or .sh on Linux).

- On **Windows** operating systems, you can alternatively use the Windows Services to control the OMM Application Server by using the `RestartApplicationService.bat` utility instead. This utility will create the Windows Service for the OMM Application Server, if it was not already created by previous execution of this utility or the `Setup.bat` utility. At this point, you can simply use the Windows Services to start, stop or restart the OMM Application Server automatically.
When running the OMM Application Server as a Windows Service, it is important to configure the user running such service in order to have full access rights to the needed files and applications. For example, the MIMB bridges involved in the metadata harvesting may need to invoke the SDK of third party software such as the COM based API of CA ERwin, or SAP BusinessObjects Universe Designer.
In order to set such access rights, go to the services manager of Windows, right-click on the OMM Application Server service. Then, go to the "Log On" tab to define an account by name under which the service will run.
- On **Linux** operating systems, administrators can use the system daemon directories (e.g. `/etc/init.d` or `/etc/systemd/`) to control the OMM Application Server (either using the `RestartApplicationServer.sh` utility or directly controlling the tomcat server in the home directory).

The final initialization steps of the setup are performed over the web browser as follows:

1. Connection

Connecting to the server on Windows can be simply achieved by opening the `Metadata Management` link in the home directory. In all cases, you can connect to the server using your internet browser to open by default: <http://localhost:11580/MM>. Note that the default port of this URL number may have been changed by the `Setup` utility in the section [Server Installation and Configuration](#).

2. Database

Define the connection to the previously created database (in the above steps), by providing the database type, user, password, and URL (JDBC connection). Press **Test Connection** button to verify proper database connectivity. Finally, when the pressing the **Save** button, the OMM Application Server will create all the necessary tables in the database.

3. Login

Login as "Administrator" with password "Administrator". Note that you should change that password later in the application by going to: **Tools -> Administration -> Users**

6.4 Custom integration with authentication environments

OMM is able to support three authentication methods:

1. Native Authentication, where the password is managed by the software and stored within the database.
2. LDAP Authentication, where the software does not manage or store the LDAP passwords at all. Instead, it is simply passed it through to LDAP in order to authenticate.
3. External Authentication such as Single Sign On (SSO), where the software does not perform any authentication, and leaves that responsibility to a local single sign on service managed by the customer.

In Tools->Administration->Users one may specify either:

1. Mixed Native and LDAP authentication where users may be authenticated either as native users or LDAP users
2. External authentication where the system does not perform any authentication, leaving it up to a local Single Sign On environment.

6.4.1 Native Authentication Configuration Issues

There are no specific configuration steps for Native Authentication.

6.4.2 LDAP Authentication Configuration Issues

There are no special server configuration issues for LDAP Authentication. LDAP connectivity configuration is documented in the online help.

6.4.3 Windows Authentication Issues

It is also possible to enable the Application Server to obtain authentication for users from Windows authentication via the browser (client). This way, users will automatically be authenticated if they are running from a Windows session.

To do so, one must install a third party product named Waffle (Windows Authentication Functional Framework) as an addon (see [here](#)):

1. Please ensure that all LDAP settings are correct and users are able to log into the product via LDAP authentication. LDAP connectivity configuration is documented in the online help.
2. Unzip the Waffle zip.
3. Copy all the jar files from it to `%OMM_HOME%\tomcat\lib`
4. Open `%OMM_HOME%\tomcat\conf\web.xml`. Search for "Windows authentication support". Uncomment the block following that.
5. Restart OMM.
6. You should have windows authentication enabled now. Any valid windows user will be logged in as guest by default as long as licensing allows it. If you need to get an administrator interface, you can access: `http://host:port/MM/Auth?nativeLogin` (optionally you can force a redirect to either `&redirectTo=/MM/Explorer` or `/MM/Manager`)
7. Provide connection information for the database you created above.

Note: Waffle is designed around Windows libraries and thus it is recommended that you use a Windows OS based machine as the Application Server. While it is possible to use Waffle on a Linux based machine, it will require a great deal of manual setup and compilation. Please follow the Waffle documentation for such an implementation (see [here](#)).

Note: When using Waffle on a Windows based Application Server (as is recommended) you must run it as a Windows service (not as an Application) in order for Waffle to work properly.

Note: Automatic Windows authentication will not allow one to use the browser refresh (f5) with IE 8.x when used as the client browser. Refresh will force a re-authentication on IE 8.x browsers and will not be automatically authenticated. If this occurs, the user must close all instances of the browser and start again. To avoid this issue, one must use IE 9.x or later or another approved browser (see [System requirements](#)) In addition, for Internet Explorer and Firefox, you must configure the browser at each client to support automatic Windows authentication. Please refer to the Waffle web site [here](#).

6.5 Custom integration for Secure Socket Layer (SSL) communication

Important Disclaimer: SSL is primarily used for HTTPS secure communications from the web browser clients to the OMM Server itself. Such common HTTPS setup can be fully achieved with the **Setup** utility as explained in [Server Installation and Configuration](#). The following steps are provided for illustration purpose only (manual steps), describing what the **Setup** utility already performs automatically. THEREFORE, YOU DO NOT HAVE TO PERFORM THESE STEPS BELOW.

If you want to manually install your own certificate, you must:

1. Change the referenced (in `server.xml`) connector entry parameters (`keystoreFile` and `keystorePass`) to point to the correct keystore file and password.
2. Import that certificate into the JRE that is being used by this tomcat. The default JRE is located under:
`%OMM_HOME%\jre`.
3. Use the following commands:

```
cd %OMM_HOME%\jre\lib\security
move jssecacerts jssecacerts.old
%OMM_HOME%\jre\bin\keytool -importkeystore -srckeystore {your_keystore} -keystore jssecacerts
%OMM_HOME%\RestartServerService.bat or RestartServerApplication.bat
```

After the configuration, use the default URL to Access OMM: <https://localhost:11580/MM>

Or use the ports specified in the server.xml file. For example:

```
<Connector port="11580" maxThreads="200"
           scheme="https" secure="true" SSLEnabled="true"
           keystoreFile="conf\keystore" keystorePass="changeit"
           clientAuth="false" sslProtocol="TLS" />
```

6.5.1 Configuring OMM to securely connect via HTTPS to another OMM server for Metadata Harvesting

Important Disclaimer: the following steps are needed ONLY IF you use a self signed certificate for SSL (WHICH IS NOT RECOMMENDED), AND ONLY in the case of configuring OMM to securely connect via HTTPS to another OMM server for Metadata Harvesting. Only in such exceptional use case, then the following additional steps have to be performed

In order to support HTTPS from a OMM Server acting as the "Metadata Manager" to a OMM Server acting as "Metadata Harvesting" Agent, the Administrator needs to import the trusted certificate that the OMM "Harvesting Agent" Server is using into the JRE that the OMM "Metadata Manager" server is using. The following page describes the process: <http://docs.oracle.com/javase/tutorial/security/toolsign/rstep2.html>.

The command looks like the following:

```
cd %OMM_HOME%\jre\lib\security
..\..\bin\keytool.exe -import -alias john -file YourOwnCertificate.cer -keystore jssecacerts
```

6.5.2 Configuring OMM to securely connect via LDAPS to the Enterprise Directory

In LDAP Authentication, the user password is not managed by the software and is simply passed through to the LDAP system.

Note: this password is not encrypted when communicated between the client and the server. Thus, in order to ensure encryption you may wish to specify HTTPS protocol communication, as above.

Note: this password is also not encrypted when communicated between the server and LDAP. Thus, in order to ensure encryption you may wish to also specify LDAPS protocol communication and thus use SSL to encrypt.

In order to support LDAPS, the OMM Tomcat service does not itself need to be configured to work with LDAPS for encryption of passwords. However, to enable secure SSL communication between OMM and LDAP servers the Administrator needs to import the trusted certificate that the LDAP server is using into the JRE that the OMM Application server is using. The following page describes the process: <http://docs.oracle.com/javase/tutorial/security/toolsign/rstep2.html>.

The command looks like the following:

```
cd %OMM_HOME%\jre\lib\security
..\..\bin\keytool.exe -import -alias john -file YourOwnCertificate.cer -keystore jssecacerts
```

This is an entirely different certificate from the one used by the HTTPS protocol.

6.5.3 SSL Security Vulnerabilities

Poodle is a "Man In The Middle" (MITM) vulnerability which needs to be primarily fixed server side. An attacker can trick the server into downgrading the encryption protocol used to communicate. The servers should be configured to disallow TLS fallback, or to disable SSLv3 as a valid protocol.

If Tomcat has been configured with SSL support, the customer should add the following to the connector description in the %OMM_HOME%\tomcat\conf\server.xml
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"

6.6 Security and Vulnerability Considerations

For extra security and vulnerability reasons, the Apache Tomcat bundled within OMM can be updated as follows:

6.6.1 Tomcat Upgrade To The Current Patches

For security and vulnerability reasons, make sure you apply any current patches from that version of Tomcat:

1. Check the version of Apache Tomcat that was bundled within your OMM (e.g. Tomcat 9.0.10) which is expressed in:
%OMM_HOME%\Documentation\License\MIMM-ThirdParty-LICENSES.html and
%OMM_HOME%\tomcat\RELEASE-NOTES
2. Download the latest patch version (e.g. 9.0.10) within the same major version:
<https://tomcat.apache.org/download-90.cgi>
3. Unzip in temporary directory
4. Stop Tomcat
5. Copy the lib directory from that temporary directory to the %OMM_HOME%\tomcat\lib (overwriting files if necessary)
6. Restart Tomcat

6.6.2 Tomcat Check For Allowed Referrer

For additional protection, we recommend enabling Tomcat to check for allowed referrer:

1. Edit %OMM_HOME%\tomcat\conf\web.xml
 1. Uncomment the two filter sections in the 'Checks referrer is allowed' section. The variable \${server.fqdn} will be substituted with the value of M_SERVER_FQDN in tomcat.properties
 2. Add as many init-param sections as needed to allow reference from other URLs.
2. Edit %OMM_HOME%\tomcat\conf\tomcat.properties by:
 1. Changing the M_SERVER_FQDN variable from 'localhost' to '<myMMServer.myDomain>'

7. Metadata Harvesting Model Bridge (MIMB) Setup

The Metadata Integration or Metadata Harvesting from third party databases, data modeling, data integration or business intelligence tools is performed by the integrated Meta Integration® Model Bridge (MIMB) software. By default, the installer software deploys and configures both OMM and MIMB on the same machine, where the OMM Application Server accesses the MIMB Web Services locally. MIMB can also be installed and configured as a remote MIMB Agent on another machine. This is very useful in architecture deployments where the metadata management server is:

- deployed remotely on the cloud but needs to access metadata harvesting servers (agents) locally on premise, or
- deployed on Linux but needs to access metadata harvesting servers (agents) on a Windows machine where DM/DI/BI client tools are Windows only (e.g. COM based SDK).

Essential customizations (e.g. directories, memory) of the MIMB Application Server can be performed in the following configuration file:

`%OMM_HOME%\conf\conf.properties`

Recommended customizations include:

- `M_BROWSE_PATH` to browse local and mapped network drive.

All metadata harvesting file and directory parameter references are relative to the server. The reason is that the server must have access to these resources anytime another event (e.g., scheduled harvest) is to occur. When harvesting a model, then, the UI presents a set of paths that may be browsed in order to select these files and directories. Setting the `M_BROWSE_PATH` parameter allows one to define which drives and network paths will be available in the UI. One may update the `M_BROWSE_PATH` using the UI (on the application server) presented by the `setup.bat` (or `setup.sh` on Linux) command (see also [Application Server Execution and Initialization](#)), or by editing the `%OMM_HOME%\conf\conf.properties` file directly.

On installation, the set includes all directly attached drives., which is specified by an asterisk `**` (`M_BROWSE_PATH=*`).

Note for Windows based application servers: When running as a service, the drive names (mapped) and paths may not be the same as what a user sees when logged in, and thus the `**` value will not be see all drives you might expect when selecting drives using the UI. Instead, one must explicitly list all the drives and network paths that one wants to be available to all users in the UI. Also, it is not sufficient to simply enter the mapped drive id (e.g., `"N:\\"`), as that drive mapping is also generally not available to services. Thus, one should specify the physical drives by letters, but must specify the network paths completely, e.g.:

`M_BROWSE_PATH=C:\, E:\, \\network-drive\shared\`

Note that the above also applies even to script backup and restore drives.

- `M_DATA_DIRECTORY` to relocate the data such as the log files, and metadata incremental harvesting cache as needed for very large DI or BI tools.
- `M_JAVA_OPTIONS` to increase the maximum memory used by java bridges during the metadata harvesting of very large DB, DI or BI tools. Note that this parameter defines the default maximum for all java bridges, however most memory intensive java bridges (e.g JDBC bridges) have the ability to define its own maximum memory in their last parameter called `Miscellaneous`.

When the MIMB Application Server is used a local metadata harvesting agent connected to a OMM Application Server on the cloud, the additional customizations are needed in the following configuration file:

`%OMM_HOME%\conf\agent.properties`

- `M_SERVER_URL` is the URL of the OMM Application Server on the cloud such as `http://server:19980/MM`
- `M_AGENT_NAME=` is the agent name such as `MyCompanyOnPremise` that the above OMM Application Server will then use to refer to this metadata harvesting server agent

8. User Interface Look & Feel Customization

8.1 Login and Headers

Customize the following files and directories using the embedded instructions (in comments):

`%OMM_HOME%\conf\resources\MM.properties`
`%OMM_HOME%\conf\resources\web\`

8.2 Metadata Explorer for Business Users

Customize the following files using the embedded instructions (in comments):

`%OMM_HOME%\conf\resources\MetadataExplorer.xml`

9. REST API SDK

The REST API SDK documentation is available within the UI by going to the Help menu (top right corner) under Help on REST API, or go directly to: <http://localhost:11580/MM/REST-API/>.

For illustration purpose, a glossary definition search demo is also available at <http://localhost:11580/MMGlossaryClient/>. This demo assumes a server URL located at "http://localhost:19980", and a glossary in a configuration called "Published". REST API application developers are familiar with the above documentation, and can find the demo source code in Chrome > top right menu > More tools > Developer tools.

10. Database Server Backup/Restore

The OMM Application Server requires the connection to an existing Database server for metadata storage (metadata repository). Metadata Integration recommends to backup the OMM metadata repository regularly and especially before any upgrade.

This document describes the commands and instructions to perform the OMM repository database backup and restore tasks. These database commands and instructions assume the following by default:

- Database Name: MM
- database User: MM

- Database Password: MM123!

The database name and user name can be changed, and the password should of course be different.

We assume that objects from backup are restored into the same database later.

Always use the same database software version to perform the backup and restore. Backups created by more recent version of a database server may not be restored in earlier versions of the database server.

Note that any data that is saved after a backup is done will be lost if you restore the backup.

Stop the OMM Application Server before you perform the backup and restore tasks. Restart the OMM Application Server afterwards.

To ensure the optimal OMM Application Server performance after a restore operation, run the database maintenance script in the OMM Management UI using Tools → Administration → Schedules → Run Database Maintenance to update the database statistics.

Backup and restore on a very large OMM repository database may take a long time. Refer to the database backup and restore documentation to enable parallelism, incremental backup and restore for better performance. The instructions given below are for a full database backup and restore.

10.1 Database on Oracle

We can use the Oracle Data Pump technology for Oracle 10g, 11g and 12c database.

First create an Oracle directory BACKUP_DIRECTORY that points to an operating system directory on the database server machine for reading and writing files.

Assume ORCL is the database server name or SID.

```
Sqlplus.exe / as sysdba
CREATE OR REPLACE DIRECTORY BACKUP_DIRECTORY as 'E:/Databases/Backups/Oracle';
GRANT read, write ON DIRECTORY BACKUP_DIRECTORY TO MM;
```

Then use Oracle Data Pump (expdp, impdp) to backup and restore the OMM metadata repository.

Backup

To backup (export) the OMM metadata repository database to a file MM.dmp and write the export log to expdpMM.log in the operating system directory E:/Databases/Backups/Oracle:

```
expdp MM/MM123! schemas=MM directory=BACKUP_DIRECTORY dumpfile=MM.dmp logfile=expdpMM.log
```

Restore

Before you restore the backup to the OMM repository database, you need to drop the schema MM to delete existing objects and data from the OMM repository database. Restore will recreate the schema MM.

```
Sqlplus.exe SYS@ORCL as SYSDBA
DROP USER MM CASCADE;
```

To restore (import) the OMM metadata repository database from a file MM.dmp and write the import log to impdpMM.log in the operating system directory E:/Databases/Backups/Oracle:

```
Impdp schemas=MM directory=BACKUP_DIRECTORY dumpfile=MM.dmp logfile=impdpMM.log
```

When prompted for Username, enter / as sysdba.

You may refer to the Oracle Data Pump documentation for more details on the expdp and impdp commands. Backup Restore using Recovery Manager (RMAN) You may also use the Oracle Recovery Manager (RMAN) to backup and restore your OMM repository database. It is a good practise to create a separate table space for OMM repository database and restore only from that table space. For more information refer to the Oracle Database Backup and Recovery User's Guide.