Oracle® Data Relationship Management Suite

Installation Guide

ORACLE®

Oracle Data Relationship Management Suite Installation Guide, Release 11.2.x

F81256-01

Contents

4   Deploying and Configuring the Data Relationship Management Web Services API

5   Installing and Configuring Data Relationship Management Analytics

6   Upgrading a Data Relationship Management Installation

7   Monitoring Data Relationship Management Applications

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Documentation Feedback

To provide feedback on this documentation, click the feedback button at the bottom of the page in any Oracle Help Center topic. You can also send email to epmdoc_ww@oracle.com.

1
About Data Relationship Management Suite

Oracle Data Relationship Management Suite consists of:

- Oracle Data Relationship Management
- Oracle Data Relationship Management Read Only Access
- Oracle Data Relationship Steward
- Oracle Data Relationship Governance
- Oracle Data Relationship Management Analytics
- Oracle Data Relationship Management for Oracle Hyperion Enterprise Planning Suite
- Oracle Data Relationship Management for Oracle Hyperion Financial Close Suite

2
Installing Data Relationship Management

Related Topics

- [Installation Prerequisites](#)
- [Additional Documentation](#)
- [About Middleware Home and EPM Oracle Home](#)
- [Foundation Services](#)
- [Installing Data Relationship Management](#)
- [Installing Data Relationship Management in a Distributed Environment](#)
- [Troubleshooting](#)

Installation Prerequisites

> **Note:**
>
> Installation instructions for Release 11.2.x are available in *Oracle Data Relationship Management Readme* .

Items to check:

- Oracle Data Relationship Management must be installed by a user who is logged in as an administrator. Installers should select to Run As Administrator when launching an installation executable.

- Intended host computers meet or exceed the minimum system requirements.

> **Note:**
>
> For information on certified versions of platform components, refer to the *Oracle Enterprise Performance Management System Certification Matrix* posted on the Supported System Configurations page on Oracle Technology Network (OTN):
>
> https://www.oracle.com/middleware/technologies/bi-foundation/hyperion-supported-platforms.html

- Microsoft .NET Framework 4.7.2. If the .NET Framework is not installed and you do have an internet connection, then the Data Relationship Management installer will install it for you.

- Database server is installed and running on the database computer.

- If the repository is set up on an Oracle database, then it should be configured with these NLS_DATABASE_PARAMETERS:

Parameter	Value
NLS_NCHAR_CHARACTERSET	AL16UTF16
NLS_CHARACTERSET	AL32UTF8

- Internet Information Services (IIS) is installed and operational on the Web server. You must include ASP.NET 4.7 support for Data Relationship Management applications to function properly.

> **Note:**
>
> MaxFieldLength and MaxRequestBytes need to be set to 32 KB.

- User accounts that can perform these actions are available on the application server:
    - Edit registry settings
    - Read and write to the local file system
    - Launch processes
    - Run as a service

PDF Font Requirement for Asian Glyphs

To provide multi-language font support for the Download to PDF option in the Data Relationship Management client, the system font "Arial Unicode MS" font must be installed on all Data Relationship Management IIS servers.

Virtual Memory Pagefile Sizing

To ensure proper performance, it is strongly recommended that Windows pagefile size on the Data Relationship Management server be at least 1.5 times system memory with growth allowed up to 2.0 times system memory. When system memory is large (for example, 64 GB and higher) the pagefile can be between 1.0 and 1.5 times system memory. Smaller pagefile sizes can result in serious performance and functional issues.

Oracle Managed Files

Database environments that allow Oracle Managed Files only require CREATE TABLESPACE commands that do not specify a filename when using the DATAFILE directive.

When installing Data Relationship Management in these environments, the tablespace must be manually created before running the Data Relationship Management Repository Wizard. Then, the already-created tablespace names need to be specified when you define the tablespace for the Data Relationship Management application in the Repository Wizard.

As an alternative, you can use the Data Relationship Management Console Repository Wizard to run SQL manually. But the generated SQL must have CREATE TABLESPACE commands that have only the DATAFILE directive with no filename specified, allowing the Oracle RDS to auto-complete the filename value.

You can omit the filename value from these SQL commands by performing either of these tasks:

- Leave the filename fields blank in the Repository Wizard screen where Tablespace options are entered.

- Review and edit the generated SQL as necessary.

HTTP Quality of Service Issues

The Data Relationship Management Client delivers a rich user experience via web browser over HTTP. For customers running the Data Relationship Management Client over a network with extremely high latency, high hop counts, or other low HTTP quality of service, it may be necessary to deliver the Client via browser sessions hosted on a Citrix Server, RDP gateway server, or other comparable UI hosting solution within the Data Relationship Management datacenter to mitigate networking issues.

Architecture Options

The following diagrams depict different scenarios for configuring Oracle Data Relationship Management.

> **Note:**
>
> EPM Foundation must be installed on a Windows server accessible by Data Relationship Management. It can be run locally or on FMW App Server.

Figure 2-1   Data Relationship Management Standard Architecture
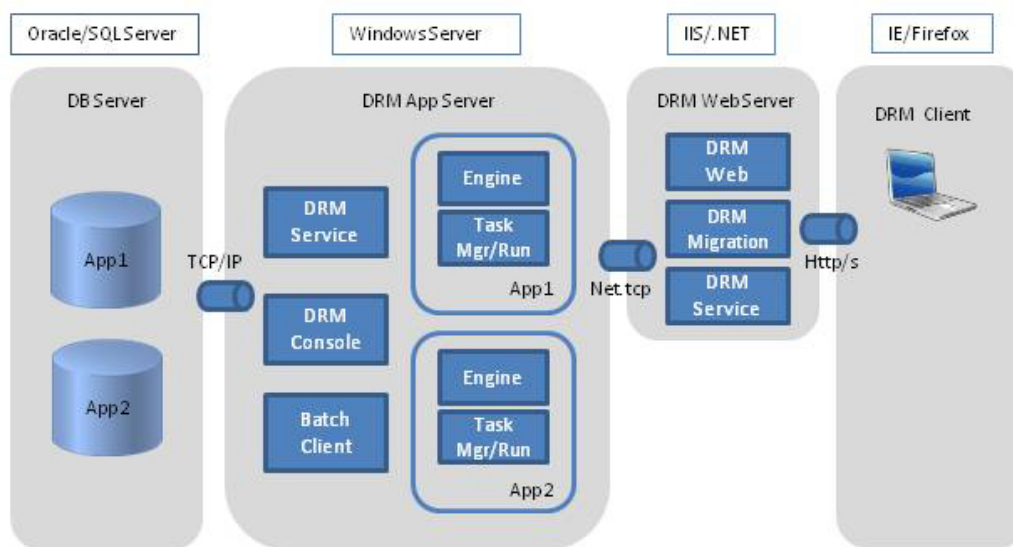
Figure 2-2   Data Relationship Management with EPM Foundation
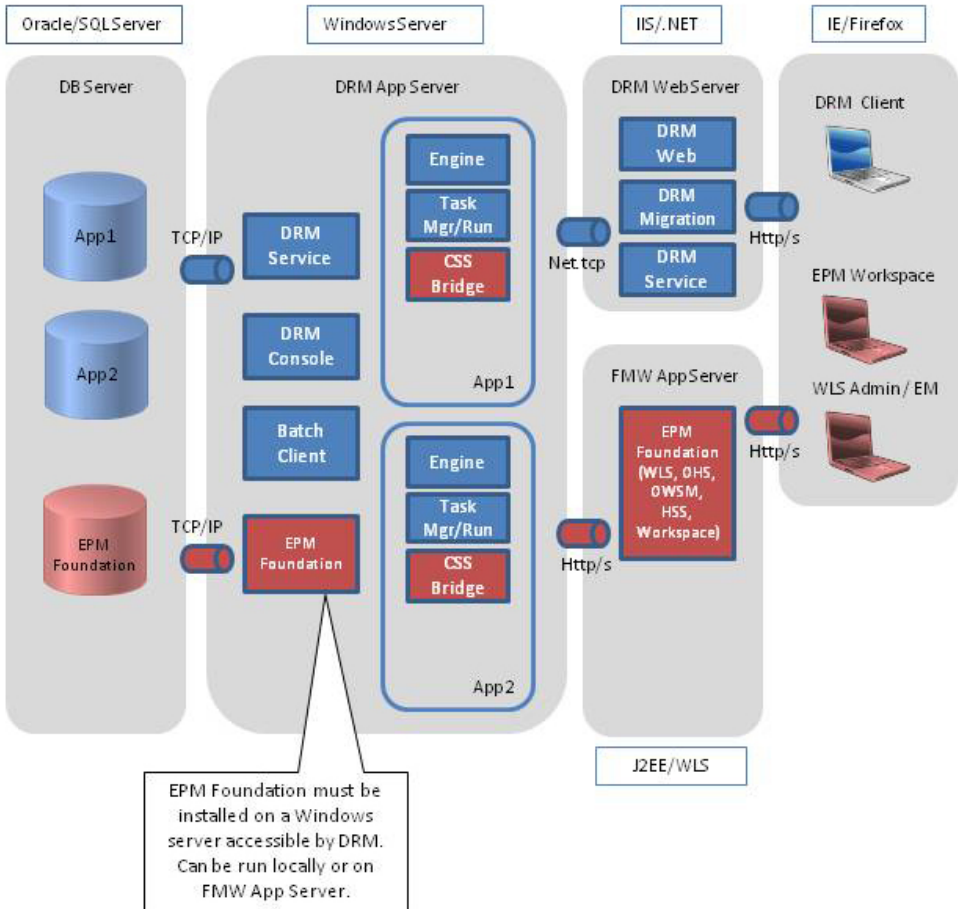
Figure 2-3   Data Relationship Management with API Integrations
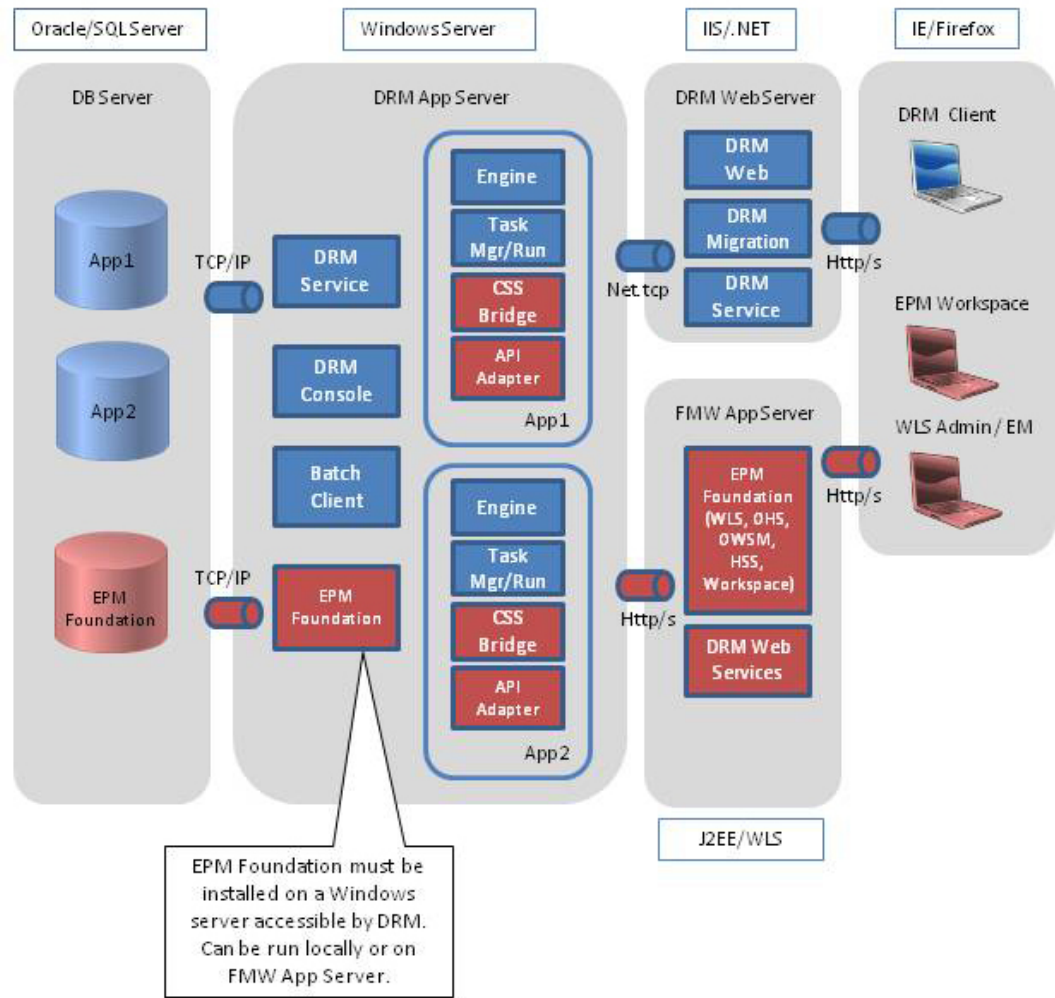
Figure 2-4   Data Relationship Management with DRM Analytics
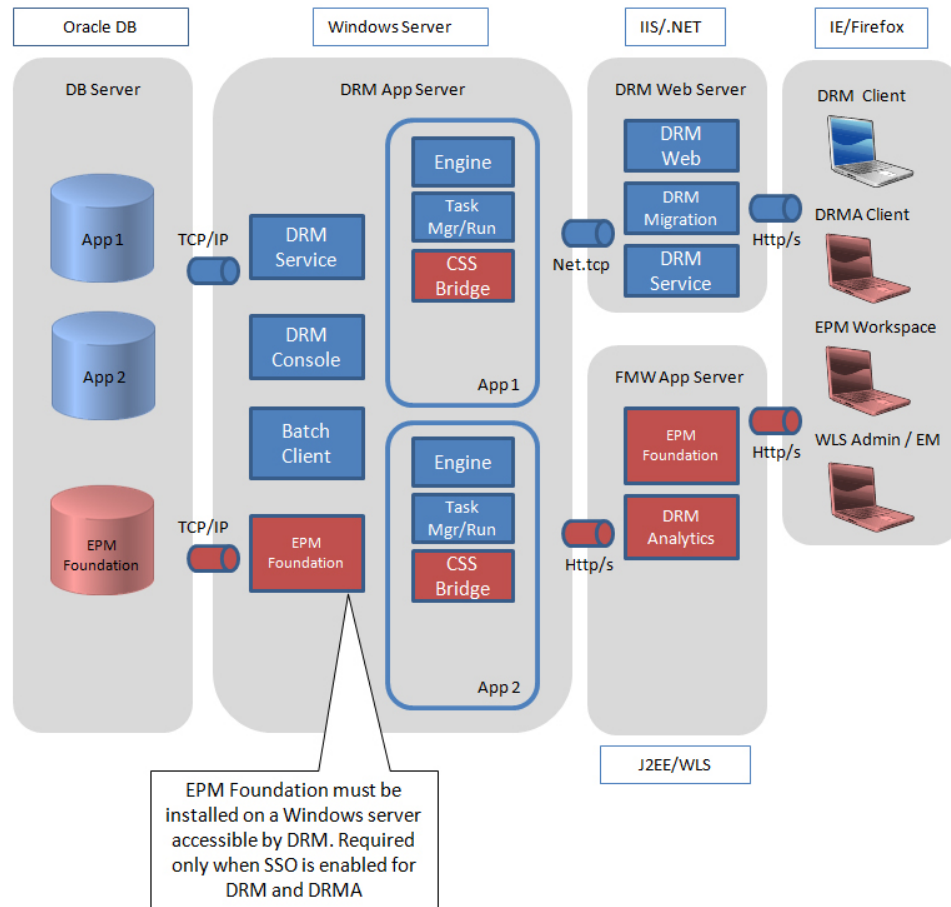
Oracle Database Installation Prerequisites

- The Oracle Data Relationship Management schema account requires access to ROLE_ROLE_PRIVS for database export external connections.

- If you are using an Oracle RAC database system, you must create the tablespaces with the appropriate RDBMS software prior to installation.

- A unique repository (and hence, schema) is required for each Data Relationship Management application.

- Oracle recommends customers use dedicated tablespaces for each Data Relationship Management schema

- Regarding repository creation, the database installation scripts are initiated via the Repository Wizard in the Data Relationship Management console which provides two options:

    - The Repository Wizard can generate the Data Relationship Management Repository (tablespaces, schema user/grants, tables and other objects) if appropriate credentials are provided

- The Repository Wizard can generate scripts that a database administrator can use to create the tablespaces, schema user/grants, tables and other objects interactively via a tool such as Oracle SQL Developer.

- Existing SYSTEM (or its equivalent) credentials are used for the first part of the script and need to be entered in the Repository Wizard.

- You will define the schema owner name and password in a later stage of the Repository Wizard.

- When specifying the account to use via the Repository Wizard where you do not intend to hand the scripts off to a database administrator to create the repository, the initial database account needs sufficient rights to create tablespaces and create and grant privileges to the schema owner that will be created. These privileges are used later in the second part of the repository creation routine to create tables, indexes, views, stored procedures, etc., and populate them with minimal configuration data for the system to start. Typically, the Oracle SYSTEM user (or an account with equivalent privileges and rights) is used for such a task. More specifically, the rights generally needed are:

  - Run a database script

  - CREATE TABLESPACE

  - CREATE SCHEMA (CREATE USER)

  - This account also must have enough privileges to perform the following Grants to the user/schema it will be creating:

    * CREATE SESSION

    * CREATE TABLE

    * CREATE VIEW

    * CREATE PROCEDURE

    * CREATE TYPE

    * CREATE SEQUENCE

    * UNLIMITED TABLESPACE for the schema owner that will be created.

    The account also needs sufficient rights to run a database script. Check with your database administrator resources regarding specific questions as many organizations choose to establish their own policies regarding account rights.

  - During this part of the Repository Creation routine, specific Repository objects and artifacts will be created using the schema owner that is used to connect to the Data Relationship Management repository by the Data Relationship Management service and application in the Data Relationship Management Console.

- When intending to create only the database scripts and hand them off to a database administrator to create the tablespaces, schema, and repository objects, the database administrator can determine the correct account(s) to use and assign the necessary privileges as part of their activity in line with the guidance above.

See Creating a Repository for more information.

> **Note:**
>
> The database accounts needed for repository and schema creation may differ based on how your organization chooses to manage their Oracle Database instance(s). Check with your database administrator if you have questions.

> **Note:**
>
> You may be able to lesson some of the Grants mentioned for the schema owner during normal service operation; however, the product is only supported and certified to be run with the default grants. If schema owner Grants are lessened, the default Grants must be re-established if at a future point a release upgrade (uninstall one release/install an updated release) and/or an "Apply Updates" is attempted.

> **Note:**
>
> While UNLIMITED TABLESPACE may not technically be required, it is a standard practice. This allows organizations to minimize the maintenance activity required on the database/schema. If the database is continually or periodically using resources to expand one or more of the required tablespaces and/or index growth/maintenance, application performance may suffer. Further, if any resources required are not made available within application timeout periods, the application may become temporarily unusable during this period. Therefore, the Data Relationship Management service and application(s) may need to be restarted once sufficient database resources are made available.

> **Note:**
>
> If you want to alter the "QUOTA UNLIMITED" directives for the schema, we suggest you first monitor Data Relationship Management usage in a non-production environment to assist with the degree of quota and database growth rates that will be necessary moving forward.

SQL Server Database Prerequisites

- If you are using a SQL Server Cluster database system, you must create the database with the appropriate RDBMS software prior to installation.
- If the User ID designated for Oracle Data Relationship Management database connectivity is created manually prior to the installation, it is important to make this user database owner of the Data Relationship Management database.

- Ensure that the MSSQL database is set up for SSL/Transparent Security if you intend to use the feature.

Additional Documentation

You can find Oracle Enterprise Performance Management System installation documentation in the Oracle Documentation Library on the Oracle Technology Network. The following documentation may be useful for installing and configuring Oracle Data Relationship Management :

- *Oracle Enterprise Performance Management System Installation Start Here*
- *Oracle Enterprise Performance Management System Installation and Configuration Guide*
- *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide*
- *Oracle Enterprise Performance Management System Backup and Recovery Guide*
- *Oracle Enterprise Performance Management System Security Configuration Guide*

About Middleware Home and EPM Oracle Home

Middleware Home

A Middleware home consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes, including EPM Oracle home. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through Network File System (NFS).

The Middleware home location is defined during the first product installation on the computer. Subsequent installations on the computer use the previously defined location. The default installation directory is `Oracle/Middleware`. The Middleware home location is referred to as `MIDDLEWARE_HOME` throughout this document.

EPM Oracle Home

An Oracle home contains installed files necessary to host a specific product, and resides within the directory structure of the Middleware home. The EPM Oracle home contains files for EPM System products.

Components of EPM System products are installed in the EPM Oracle home directory under the Middleware home. The default EPM Oracle home location is `MIDDLEWARE_HOME/EPMSystem11R1`. In addition, common internal components used by the products are installed in EPM Oracle home. Choose the location carefully to ensure that the location has enough disk space for all products that you are installing on the machine. You cannot change the location.

The EPM Oracle home location is defined in the system environment variable called `EPM_ORACLE_HOME` . The EPM Oracle home location is referred to as `EPM_ORACLE_HOME` throughout this document.

Foundation Services

Oracle Data Relationship Management requires Oracle Hyperion Foundation Services to be installed when the following optional features are used:

- User authentication with external user directories such as LDAP.

- Load balancing Data Relationship Management Web applications

- Using single-sign on with Data Relationship Management

- Integrations with Oracle General Ledger for E-Business Suite and Fusion Accounting Hub

- API programs and SOA-based processes using the Data Relationship Management web service

The Foundation Services installation includes the following components which can be configured to enable these features for Data Relationship Management:

- Oracle WebLogic Server

- Oracle HTTP Server

- Oracle Web Services Manager

- Oracle Hyperion Shared Services

Foundation Services is installed using the EPM System installer. The installation and configuration process for Foundation Services is documented in the *Oracle Enterprise Performance Management System Installation and Configuration Guide* .

Data Relationship Management CSS Bridge

The Oracle Data Relationship Management CSS Bridge is used to communicate with Oracle Hyperion Shared Services and must be installed when Oracle Hyperion Foundation Services is used with Data Relationship Management. The following information and requirements are important for understanding the Data Relationship Management CSS Bridge.

- The CSS Bridge Host system can be the Data Relationship Management application server or a different supported Microsoft Windows system.

> **Note:**
>
> The CSS Bridge component is not supported on Unix/Linux systems.

- If the designated CSS Bridge Host is not the Data Relationship Management application server, then the CSS Bridge component must be installed on the CSS Bridge Host. In this scenario, the CSS Bridge can be installed as a standalone component.

- A Foundation Services installation and deployment is required on the Windows system where the CSS Bridge will be installed and running.

For CSS Bridge deployment options, see Deployment Scenarios for Data Relationship Management and Foundation Services.

Deployment Scenarios for Data Relationship Management and Foundation Services

Review Figure 2 for more information on Oracle Data Relationship Management with Oracle Hyperion Foundation Services. See Configuring Secondary Foundation Services Hosts.

> **Note:**
>
> All systems are Microsoft Windows unless otherwise noted.

Table 2-1   Deployment Scenarios for Data Relationship Management and Foundation Services

Scenario	System 1	System 2	System 3
1	• Windows Data Relationship Management application server • Windows primary Foundation Services instance • Windows Data Relationship Management CSS Bridge	N/A	N/A
2	Windows Data Relationship Management application server	• Windows primary Foundation Services instance • Windows Data Relationship Management CSS Bridge	N/A
3	• Windows Data Relationship Management application server • Windows secondary Foundation Services instance • Windows Data Relationship Management CSS Bridge	Windows primary Foundation Services instance	N/A

Table 2-1   (Cont.) Deployment Scenarios for Data Relationship Management and Foundation Services

Scenario	System 1	System 2	System 3
4	• Windows Data Relationship Management application server • Windows secondary Foundation Services instance • Windows Data Relationship Management CSS Bridge	Unix/Linux primary Foundation Services instance	N/A
5	Windows Data Relationship Management application server	Unix/Linux primary Foundation Services instance	• Windows secondary Foundation Services instance • Windows Data Relationship Management CSS Bridge

Installing Data Relationship Management

> **Note:**
>
> The Oracle Data Relationship Management installer requires Run As Administrator rights in order to execute properly.

Before installing Data Relationship Management, review Architecture Options.

To install Data Relationship Management:

1. Navigate to the directory where you downloaded the installation program, right-click `setup.exe` and select **Run as administrator**.

2. Select the language for the installation and click **OK**.

3. If you do not already have Microsoft .NET Framework 4.7.2 installed, click **Install** to install it.

> **Note:**
>
> You must have an internet connection for the .NET installation to complete.

4. On the **Welcome** dialog box, read the license agreement and click **Next**.

5. Click **Next** to accept the default installation directory for Data Relationship Management files, or click **Change**, select an installation location and then click **Next**.

6. On the **Setup Type** dialog box, select the type of installation to perform and click **Next**:

    • **Complete** — Installs the Application Server, CSS Bridge, Web Server, Migration Utility, and Batch Client.

    • **Custom** — Allows you to select the components to install. You can select from the following components:

        – DRM Application Server—Core engine and server files

        – DRM CSS Bridge—Data Relationship Management connector for Oracle Hyperion Shared Services

        – DRM Web Server—Primary Web application for Data Relationship Management users

        – DRM Migration Utility—Web application for managing application templates

        – DRM Batch Client—Windows console client for running batch operations

7. Do one of the following:

    • If you selected **Complete**, skip to the next step.

    • If you selected **Custom**, on the **Custom Setup** dialog box select the features to install and click **Next**.

    > **Note:**
    >
    > All features are selected by default. Deselect the features that you do not want to install.

8. Click **Install**.

9. Click **Finish**.

    > **Note:**
    >
    > To create and configure Data Relationship Management applications, select the option to launch the Data Relationship Management Configuration Console.

Installing Data Relationship Management in a Distributed Environment

Installing Secondary Data Relationship Management Web Server Hosts

To install a secondary Oracle Data Relationship Management Web Server computer, install the Data Relationship Management Web Server component on the secondary computer. See Configuring Foundation Services for Data Relationship Management.

Installing Secondary Foundation Services Hosts

The following Oracle Hyperion Foundation Services components must be installed on the secondary Foundation Services instance using the EPM System Installer:

- Foundation Services Web Applications
- Static Content Files
- WebLogic Application Server

Troubleshooting

For information on installation troubleshooting, see the *Oracle Enterprise Performance Management System Installation and Configuration Troubleshooting Guide* .

3
Configuring Data Relationship Management

The Oracle Data Relationship Management Configuration Console is an application server configuration utility and is installed automatically when you install the application server component. You can open the console at the end of the installation program.

> **✎ Note:**
>
> All Data Relationship Management servers and related servers must be configured to actively synchronize to a common time source on the network. Unsynchronized servers will lead to Web Services failures for packaged integrations and other Data Relationship Management API usage. It will also increase the complexity for deployment and operation of Data Relationship Management with its partner systems.

> **⚠ Caution:**
>
> All Data Relationship Management servers and related servers must be configured to use the same keystore in the same path on every server.

Configuring Foundation Services for Data Relationship Management

The Oracle Hyperion Foundation Services installation includes several components which must be deployed and configured using the EPM Configurator tool before Oracle Data Relationship Management can use them.

See the "Configuration Sequence" section of the *Oracle Enterprise Performance Management System Installation and Configuration Guide* for information on the order in which components should be configured. Refer to the "Configuring EPM System Products" section for instructions for performing the configuration of Foundation Services components.

Configuring Shared Services for Single Sign On (SSO)

See "Configuring EPM System for SSO" in the *Oracle Enterprise Performance Management System Security Configuration Guide* .

Configuring CSS Mode for Data Relationship Management

The Data Relationship Management server must be configured for CSS Authentication mode or Mixed mode in order to authenticate users using Oracle Hyperion Shared Services. See Configuring the CSS Bridge and Configuring Authorization Policies.

Configuring Secondary Foundation Services Hosts

- The Windows Oracle Data Relationship Management service must be started and running on the CSS Bridge Host computer before starting the Data Relationship Management service on the application server.

- If a secondary Oracle Hyperion Foundation Services instance is utilized for the CSS Bridge, then:

  – The following Foundation Services components must be configured on the secondary Foundation Services instance using the EPM System Configurator:

    * Configure Common Settings

    * Configure Oracle Configuration Manager

    * Configure Database

    * Deploy to Application Server

  – For the *Select the EPM Oracle Instance to which the configuration would be applied* configuration, use the default or custom path for *Home directory for EPM Oracle instances*; use the default for *EPM Oracle instance name*.

  – For the *Set up Shared Services and Registry Database associated with the instance home* configuration, select the *Connect to a previously configured Shared Services database* option, and provide the connection information for the database configured for the primary Foundation Services instance.

  – For the *Deploy to Application Server/Specify WebLogic Domain* configuration, select the *Deploy Web applications to a new domain* option.

  – After installation and configuration, the EPM Web Application Server does not need to be started or running on the secondary computer.

See Data Relationship Management CSS Bridge.

Configuring Shared Services with an External Provider

To configure Oracle Hyperion Shared Services, see "Configuring OID, Active Directory, and Other LDAP-based User Directories" in the *Oracle Enterprise Performance Management System User Security Administration Guide* .

For development purposes, Shared Services can be configured to use the WebLogic embedded LDAP server as an external directory. For information, go to: http://www.oracle.com/technetwork/middleware/bi-foundation/resource-library-090986.html and select **EPM System Tips & Tricks 1-72 (PDF)**. In that document, see "Is it possible to use the WebLogic embedded LDAP server as an external directory for EPM System 11.1.2 products?".

Configuring Shared Services with Data Relationship Management User Roles

You add Oracle Data Relationship Management roles in Oracle Hyperion Shared Services by running one of the SQL scripts provided with the Data Relationship Management installation.

To add Data Relationship Management roles in Shared Services:

1. On the server where Data Relationship Management is installed, navigate to the server\config folder, which is typically:

   `C:\Oracle\Middleware\EPMSystem11R1\products\DataRelationshipManagement\server\config.`

2. Run the appropriate SQL script for the Shared Services database which was configured in the EPM configuration process: `drm_roles_oracle.sql` or `drm_roles_sql_server.sql`.

   a. Log into the database server as a user with database administrator privileges.

   b. Run the script against the Shared Services database.

Configuring Data Relationship Management Applications for TCPS

Oracle Data Relationship Management applications can be configured in the Configuration Console for the DRM Repository to exist on an Oracle (19c) database, set up with TCPS. To apply this configuration, a new feature has been added to the **Configuration Console**. This feature now allows you to select the option **Use SSL/TCPS**.

To configure Oracle Data Relationship Management Applications for TCPS:

1. Open the Data Relationship Management Configuration Console by selecting **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, and then **Configuration Console**.

2. Select **Use SSL/TCPS**. This will present an additional text box below **Service Connection**, where you can specify a Wallet Location.

3. Click **Save Configuration**.

The Wallet Location (for example, `c:\ssl`) is the location (path) for the SSL Certificates\wallet files that needs to be imported from the database server. These typically include:

- Root Cert (ca.crt, for example)
- Intermediate Cert (intermediate.crt, for example)
- cwallet.sso
- ewallet.p12

Note: Ensure that the certificates exist in the Wallet Location before you enable the **Use SSL/TCPS** check box.

Configuring Data Relationship Management Applications for MSSQL Server SSL

Oracle Data Relationship Management applications can be configured in the Configuration Console for the DRM Repository to exist on an MSSQL set up with Secure Connections. To apply this configuration, a new feature has been added to the **Configuration Console**. This feature now allows you to select the option **Use SSL/TLS**.

To configure Oracle Data Relationship Management Applications for MSSQL Server SSL:

1. Open the Data Relationship Management Configuration Console by selecting **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, and then **Configuration Console**.

2. Select **Use SSL/TLS** and configure the connection information and credentials.

3. Click **Save Configuration**.

Starting the Data Relationship Management Configuration Console

To open the Oracle Data Relationship Management Configuration Console, select **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, then **Configuration Console**.

Configuring Data Relationship Management Applications

Oracle Data Relationship Management uses applications to manage data and serve user requests for accessing data. You can run one or more Data Relationship Management applications on a single machine. Each application and repository can be accessed by only one active instance of Data Relationship Management application server.

Before configuring multiple Data Relationship Management applications, review Figure 1.

Creating an Application

Oracle Data Relationship Management applications are created in the Configuration Console. At least one application must be created.

To create a Data Relationship Management application:

1. In the Data Relationship Management Configuration Console, click **Add** to create a new application.

2. On the **Configuration** tab, configure the repository.

3. Click **Save Configuration**.

4. From the **Local Service** menu, click **Start** to start the Data Relationship Management service.

When you add a new application, the application is created with standard default parameters. The default application name is generated from the computer name.

> **Note:**
>
> The single quote character is not a supported character for Application and/or Repository names. Oracle suggests that you limit the names of Data Relationship Management Applications and/or Repositories to alphanumeric characters and the underscore character.

Setting the Application Default Culture

You can set the default culture used for each Oracle Data Relationship Management application. The default culture is used for localization of the Web client if the setting cannot be determined from the Web browser.

To set the default culture for an application:

1. In the Data Relationship Management Configuration Console, select an application.

2. From Default Culture select an option:

   - en-US – English

   - fr-FR – French

   - de-DE – German

   - ja-JP – Japanese

   - ko-KR – Korean

   - zh-CHS – Simplified Chinese

Date, Time, and Number Formatting

Date and time values are formatted in the invariant culture. This allows for a predictable response and action can be taken to re-format the result, if desired.

Formatting of number property data values in the Oracle Data Relationship Management user interface is determined by two factors:

- The language setting of the Data Relationship Management client computer's browser

- The Regional Options settings defined for the Data Relationship Management service logon account on the Data Relationship Management application server computer.

The Data Relationship Management Web Client session information includes the user's culture as defined in the browser's language setting. The data value formatting displayed at the client for the requested culture is determined by how the corresponding culture formatting is defined on the Data Relationship Management server for the Regional Options of the DRM service logon account. The client operating system's Regional Options settings do not affect data formatting in the user interface.

Similarly, the Data Relationship Management Batch Client parameter "/CultureName" allows you to specify the culture format as you would via the browser language. And as with the Web client, the data value formatting is determined by how the corresponding culture is defined on the Data Relationship Management server for the Data Relationship Management service logon account.

> **Note:**
>
> The default logon account for the Data Relationship Management Server Processes service is "Local System". To view or customize the Regional Options used by Data Relationship Management, the Data Relationship Management service logon account should be changed from Local System to a local Administrator account. This enables you to log onto the server as the service account and view or modify the Regional Options that the Data Relationship Management service uses.

Creating a Repository

The Repository Wizard in the Configuration Console allows you to create a new repository or upgrade a repository.

> **Caution:**
>
> Each Oracle Data Relationship Management application needs it own repository. Two applications should never be configured to use the same repository.

> **Note:**
>
> Depending on the configuration of the network, DNS setup and IPv4/IPv6 configuration and localhost settings, and since these settings vary widely across implementation topologies, it may be necessary to set up the Data Relationship Management service connection to the repository using the appropriate Fully Qualified Domain Name or the static IP address and the database service identifier.

To create a new repository:

1. Click the **Repository Wizard** button.

2. Select **Create a new repository**.

   - **Optional:** Select **Estimate size based on existing repository** to create a new repository based on the size of an existing repository.

   - **Optional:** Select **Generate SQL scripts** to create and download database creation scripts to run at a later time

3. Click **Next**.

4. Do one of the following:

   - If you are generating scripts, go to Generating SQL Scripts.

   - If you selected any other option in the previous step, continue to the next step.

5. Do the following:

- Select the database provider: Oracle or SQL Server.

- Enter the connection to the target database where the new repository will reside.

- Enter the user ID and password for an administrator who has rights to create a database schema and data files.

> **Note:**
>
> For SQL Server, only SQL accounts are supported.

- **Optional:** For **Connection Timeout**, enter the number of seconds to wait for a connection to open before canceling the attempt and generating an error. The default is 60 seconds. For **Command Timeout**, enter the number of seconds to wait for a command to execute before canceling the command and generating an error. The default is 900 seconds.

> **Note:**
>
> Setting the timeout value to zero indicates no timeout is used. These settings are saved in the `drm-config.xml` and are used by the engines when they start. To perform large operations (such as a large version delete), set the Command Timeout to a larger value than the default.

- Click **Test Connection**.

6. Click **Next**.

7. Do one of the following:

    - For an Oracle database, continue to the next step.

    - For a SQL Server database, go to Creating a SQL Server Database.

8. Enter the user id and password which will be created as the schema owner for the Data Relationship Management repository.

9. Accept the default tablespace settings or make changes and click **Next**.

> **Note:**
>
> It is highly recommended that dedicated tablespaces be used for Data, Indexes, Transactions, and Properties. The default tablespace names may already be in use, and will be re-used if a new tablespace name is not specified.

10. On the **Application Administrator Creation** page, enter a password for the Administrator user and click **Next**.

11. On the **Create Repository Confirmation** page, review the settings and click **Next** to start the creation process.

    When the database has been created a success message is displayed.

12. Click **Next**.

> **Tip:**
>
> Repository creation, copy, and upgrade information is written to the Repository Wizard log. Click **Save Log** on the **Repository Operation Complete** page of the wizard to save the log file.

13. On the **Repository Operation Complete** screen, click **Finish**.

    You are returned to the main screen of the console where you can review the settings.

    > **Note:**
    >
    > If you entered the Repository Wizard from the menu bar, Finish returns you to the first page of the wizard. If you entered the wizard from the button on the application tab, clicking Finish applies the settings to the selected application. If you click Cancel, the repository is still created, but the settings are not applied to any application. The new database is applied when you save the configuration.

14. Click **Save Configuration**, otherwise connection information is lost when the console is closed.

Creating a SQL Server Database

To configure a SQL Server database for the Oracle Data Relationship Management repository:

1. Enter the user id and password which will be created as the login for the Data Relationship Management database.

   > **Caution:**
   >
   > When creating a database user name or password, you cannot use the following symbols: at (@), slash (/), comma (,), and colon (:).

2. Enter the name of the database to create to hold the Data Relationship Management repository.

   > **Caution:**
   >
   > Database names cannot begin with a number.

3. Do one of the following and then click **Next**:

   - Select **Use server defaults for data files** to use default settings for the path to and size for the database and log file.

   - Enter the path to and size for the data file and log file.

4. On the **Application Administrator Creation** page, enter a user name and password for the Administrator user and then click **Next**.

5. On the **Create Configuration** page, review the target repository information, and then click **Next**.

> **Note:**
>
> After the repository is created, you can save the log.

6. Do one of the following:

    • Click **Finish** to apply the changes to the current application.

      You are returned to the main screen of the console where you can review the settings.

    • Click **Cancel** to exit the wizard.

7. Click **Save Configuration**, otherwise connection information is lost when the console is closed.

Generating SQL Scripts

You can generate SQL scripts from which you can manually create a repository. When you save the scripts, you are not required to provide repository connection information.

To generate SQL scripts:

1. Click the **Repository Wizard**.

2. Select **Generate SQL scripts** and click **Next**.

3. Select the **Oracle** or **SQL Server** tab and enter repository information.

4. Click **Next**.

5. On the **Repository Creation Script** screen, click **Save to File** and navigate to a folder in which to save the file.

> **Note:**
>
> The file name for both Oracle and SQL Server databases is `drm-create-database.sql.`

6. Click **Next**.

7. On the **Repository Object Creation Script** screen, click **Save to File** and navigate to a folder in which to save the `drm-create-schema-objects.sql` file.

8. Click **Next**.

9. Click **Finish**.

Manually Running Database Scripts

Based on your local security procedures, creating a new database may require a level of access that is not available to the user installing Oracle Data Relationship Management. Thus, during the installation, there is an option to save the database scripts to disk rather than running them automatically. The scripts can then be run separately by the appropriate database administrator.

To manually run scripts:

1. Log into the database server as a user with database administrator privileges.

2. Run the scripts in the following order:

    *   `drm-create-database.sql`

    *   `drm-create-schema-objects.sql`

3. After all scripts have been successfully run, open the Data Relationship Management Configuration Console.

4. Click **Add**.

5. On the **Repository Configuration** tab, enter the service connection information and click **Save Configuration**.

    > **Note:**
    >
    > You can click **Test Connection** to verify connectivity.

    This completes the manual creation of the Data Relationship Management repository.

6. Select the application from the **Applications** list.

    The database is automatically initialized the first time the application is started.

Copying a Repository

Use database tools (such as EXPDP / IMPDP) to migrate an existing repository to a new instance, configure the repository connection, and then Apply Updates.

Configuring Host Computers

Oracle Data Relationship Management server components can operate on one or more host computers. The Configuration Console enables you to configure host computers for each server component. For configuration details, refer to the applicable host computer section:

*   Configuring an Engine Host

*   Configuring the API Adapter

*   Configuring Web Servers

*   Configuring the CSS Bridge

- Configuring an SMTP Server

Configuring an Engine Host

To configure an engine host computer:

1. In the Configuration Console, select **Host Machines** and on the **Engine** tab, enter the computer name and port number.

2. For **Engine Startup Timeout**, enter the number of seconds to wait when starting a Oracle Data Relationship Management engine process.

> **Note:**
>
> If the engine does not respond within the number of seconds, an error is logged in the Windows Event Log.

Configuring the API Adapter

The API Adapter component is included with the Oracle Data Relationship Management Application Server installation component.

> **Note:**
>
> Enable the API Adapter if you are going to access Data Relationship Management using the Web Services API.

To enable the API adapter host:

1. In the Configuration Console, select **Host Machines** and then **API Adapter**.

2. Do the following:

    - Select **Enable API Adapter**.

    - Enter the port number for the host.

    - Enter the SSL certificate name.

3. Click the **Test URL** link to verify that the link is valid.

Configuring Web Servers

On the UI Web Servers tab, list the servers that are configured to run the Oracle Data Relationship Management Web client application.

On this tab, you can also:

- Configure additional Web server attributes for calculating node URLs on the **Web Farm** tab.

- Set up anonymous profiles which allow access to the Web client via a custom URL without the user having to log in on the **Anonymous Profiles** tab.

To configure Web Servers:

1. In the Configuration Console, select **Host Machines** and then **UI Web Servers**.

2. On the **Host Servers** tab, enter the name of the server(s) that are configured to run the Data Relationship Management Web client application.

> ⚠️ **Caution:**
>
> The computer name must be listed here in order for the application to be displayed in the application list for the Data Relationship Management Web client when a user logs into Data Relationship Management.

3. On the **Web Farm** tab, do the following:

   a. In **Host Name**, enter the computer name to be used for all calculated node URLs

   b. Enter the host port number.

   > 📝 **Note:**
   >
   > The default is 80.

   c. In **Path**, enter the directory application path for the Data Relationship Management logon page.

   > 📝 **Note:**
   >
   > The default is `http://localhost/drm-web-client`.

   d. Select **Uses SSL** to use "https://" computed URLs. Otherwise, "http://" is used.

   e. Click the **Test URL** link to verify that the link is valid.

4. On the **Anonymous Profiles** tab, do the following:

   a. Enter a name in the **Add Profile** text box.

   b. Click the plus sign (+) to add the profile to the list of profiles.

   c. Enter login credentials for the profile.

   d. Click **Save Profile** to validate and save the new profile in memory.

   e. Click **Save Configuration** to permanently save the profile to the Data Relationship Management configuration.

   > 📝 **Note:**
   >
   > All profiles on this tab are saved to the servers on the Host Servers tab.

   The anonymous access URL is created in this format: `http://DRM_Web_Server/drm-web-client/Logon.aspx?app=DRM_App_Name&login=Anonymous`

For example, `http://localhost/drm-web-client/Logon.aspx?app=DRMApp1&login=AnonUser1`

Configuring the CSS Bridge

To configure the CSS Bridge:

1. In the Configuration Console, select **Host Machines** and then **CSS**.

2. On the **General** tab, configure the following options:

   - **Enable CSS Bridge** – Select to enable CSS

   - **Enable SSO** – Select to enable Single Sign On.

   > **✎ Note:**
   >
   > For information on SSO, see Using Single Sign On with Data Relationship Management. For information on setting authentication settings, see Configuring Authorization Policies.

   - **CSS Bridge Host** – Enter the name of the Shared Services computer that will be running the Data Relationship Management CSS Bridge component that is required for Data Relationship Management to communicate with Shared Services. For more information, see Data Relationship Management CSS Bridge and Configuring Secondary Foundation Services Hosts.

     When properly configured, the `drm-netjnibridge-host.exe` process will be launched on the CSS Bridge Host. Refer to the Windows event logs on the CSS Bridge Host and Oracle Data Relationship Management computers to troubleshoot configuration issues.

   - **JVM Path** – The path to the java virtual machine (`jvm.dll`). Default location for 64-bit is `C:\Oracle\Middleware\jdk1.8.0_181\jre\bin\server\`**jvm.dll** .

   - **Oracle Instance** – The path for the EPM instance. Default location is `C:\Oracle\Middleware\user_projects\epmsystem1`.

   > **✎ Note:**
   >
   > All settings on the General and Class Path tabs are relative to the CSS Bridge Host computer which is not necessarily the Data Relationship Management application server.

3. On the **Class Path** tab, enter the paths to the required .jar files. These paths must be modified for the user's environment. Examples of class paths are:

   `C:\Oracle\Middleware\EPMSystem11R1\products\DataRelationshipManagement\server\jar\cassecurity.jar`

   `C:\Oracle\Middleware\EPMSystem11R1\products\DataRelationshipManagement\server\jar\drm-epm-registry.jar`

   `C:\Oracle\Middleware\EPMSystem11R1\common\jlib\11.1.2.0\epm_j2se.jar`

```
C:\Oracle\Middleware\oracle_common\modules\javax.servlet.javax.servlet
-api.jar
```

4. On the **Additional JVM Parameters** tab, add any additional JVM startup parameters that may be required, one parameter per line.

   For example, `-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true`

   > **Note:**
   >
   > The **Additional JVM settings** tab allows you to specify additional JVM launch settings that may be required in certain environments. This should be used sparingly and only when absolutely necessary. Do not attempt to override the Minimum and Maximum JVM Heap values by adding additional parameters. These are regulated by the spinner control settings on the General Tab under CSS.

Configuring an SMTP Server

The Data Relationship Governance feature uses email notifications to notify governance users and data managers of requests activities. You must enable and configure SMTP Server settings for Data Relationship Governance notifications to work.

> **Note:**
>
> An SMTP server must be set up locally or be remotely accessible by the Oracle Data Relationship Management application server.

To configure an SMTP server:

1. In the Configuration Console, select **Host Machines** and then **SMTP Server**.

2. Select **Enable SMTP**.

3. Specify the host name of the SMTP server and the port number.

4. Specify the SMTP port number.

5. **Optional:** Select **Use SSL** to use "https://" computed URLs. Otherwise, "http://" is used.

6. **Optional:** Select **Requires SMTP Authentication** and enter the user name and password for the SMTP server.

7. Enter the sender name which will display in the email From field.

8. Enter the sender email address.

Configuring Analytics URL

To be able to drill through from the Oracle Data Relationship Management Analytics module to Oracle Data Relationship Management you must configure.

To configure the Analytics URL:

1. In the Configuration Console, select **Host Machines** and then **Analytics URL**.

2. On the **Analytics URL tab** tab, do the following:

   a. In **Host Name**, enter the computer name of load balancer or web farm to use when generating URLs.

   b. Enter the host port number.

   > **Note:**
   >
   > The default is 9800.

   c. In **Path**, enter the directory application path for the Data Relationship Management Analytics component.

   > **Note:**
   >
   > The default is `http://localhost:9800/oracle-epm-drm-analytics`.

   d. Select **Uses SSL** to use "https://" computed URLs. Otherwise, "http://" is used.

   e. Click the **Test URL** link to verify that the link is valid.

Configuring Authorization Policies

On the **Authorization Policies** tab, you can select the user authentication type, modify internal authentication policies, and set lockout parameters for users.

To configure authorization policies:

1. In the Configuration Console, select **Security Settings** and then select **Authorization Policies**.

2. Click **Load Settings** to populate the current settings as saved in the Oracle Data Relationship Management system preferences.

3. Select the method for authentication:

   • **Internal** – Managed fully by Data Relationship Management.

   • **CSS** (Common Security Services) – Centralized support for external user directories using Oracle Hyperion Shared Services.

   • **Mixed** – Allows authentication option (Internal or CSS) to be specified by the user.

4. Set password preferences:

   • **Expiration Period (days)** – Number of days that a user's password is valid.

   • **Maximum Length** – Maximum length for user passwords; zero indicates no maximum.

   • **Minimum Length** – Minimum length for user passwords; zero indicates no minimum

- **Warning Period** – Positive or negative number to indicate how many days before (-) or after (+) the password expiration date to warn users to change their password before no longer allowing them to log in.

5. Set user lockout preferences:

- **Inactivity Threshold** – Maximum number of days of inactivity before a user is locked out.

- **Invalid Logins Allowed** – Maximum number of invalid log in attempts before a user is locked out.

6. Click **Save Settings**.

Configuring EPM Registry Settings

Oracle Data Relationship Management application settings must be registered in the Oracle Hyperion Shared Services EPM Registry to enable Common User Provisioning.

> **Note:**
>
> You can unregister an application by clicking Unregister. To unregister an application, the CSS Bridge must be enabled and the application that you are unregistering must be running.

To register a Data Relationship Management application:

1. Ensure that you have enabled the API adapter and CSS bridge for the Data Relationship Management application and set the authentication setting to CSS or Mixed.

   See Configuring API Adapter Hosts, Configuring the CSS Bridge, and Configuring Authentication Settings.

2. In the Configuration Console, select **EPM Registry** and then on the **Application** tab specify the Data Relationship Management Web service by providing this information:

   - HTTP or HTTPS protocol

   - Host computer name of the Web service

   - Port number

   - Application context — Name of the WebLogic application for the Web service

   > **Note:**
   >
   > This information is combined into a URL; for example, `http://servername:managedServerPort/oracle-epm-drm-webservices`
   >
   > where http is the protocol, *servername* is the host computer name of the Web service, *managedServerPort* is the port number of the managed server, and oracle-epm-drm-webservices is the name of the WebLogic application for the Web service.

3. Specify the Data Relationship Management user credentials used for the integration.

4. Click **Register**.

Configuring Common User Provisioning

The Common User Provisioning feature enables users and groups to be provisioned to Oracle Data Relationship Management applications using Oracle Hyperion Shared Services. This configuration allows Data Relationship Management users to be provisioned in a common location along with other Oracle EPM applications. Common User Provisioning also eliminates the need to separately provision users in the Data Relationship Management application. Provisioning information can be synchronized from Shared Services to Data Relationship Management on-demand or a scheduled basis. Common User Provisioning is disabled by default.

> ⚠️ **Caution:**
>
> Before enabling Common User Provisioning for a Data Relationship Management application, Data Relationship Management roles must be added to Shared Services and the Data Relationship Management application must be registered with Shared Services. See "Managing Common User Provisioning" in *Oracle Data Relationship Management Administrator's Guide* .

To enable Common User Provisioning:

1. In the Configuration Console, select **Security Settings** and then **CSS Synchronization**.

2. Select **Enable Common User Provisioning**.

To schedule daily synchronization from Shared Services:

1. In the Configuration Console, select **Security Settings** and then **CSS Synchronization**.

2. Select **Enable Common User Provisioning**.

3. Select **Auto Synchronize** and then enter a start time.

4. Enter the username and password for a user with the Shared Services Provisioning Manager role.

Configuring Scheduled Tasks

The Task Runner component handles the execution of scheduled processes which run in the background on the Data Relationship Management application server. The Configuration Console enables you to define settings for scheduled tasks.

Purging Deleted Version Records

Database records for deleted versions are permanently removed from the Oracle Data Relationship Management repository as a scheduled task. This process reduces the impact on performance of other system operations by allowing the delete process to be run during periods of low system usage. An administrator can configure frequency and blackout settings for the purge process.

To permanently delete all version-related records for versions that have been marked for deletion:

1. In the Configuration Console, select an application and then select **Scheduled Tasks**.

2. Click **Load Settings** to populate the current settings as saved in the Data Relationship Management system preferences.

3. Enter a number for the frequency of the purge and then select the unit of time as hours, minutes, or seconds.

4. **Optional:** To set a blackout window when scheduled purges should not run, enter the start time for the blackout and then select how long (in hours) the blackout should last.

5. Click **Save Settings**.

Removing an Application

You can remove an application when it is no longer useful.

To remove an application, right-click the application and select **Remove**.

Saving Configuration Settings and Starting the Service on the Application Server

Changes made in the Configuration Console must be saved and the Oracle Data Relationship Management service must be restarted for these changes to take effect.

> **Note:**
>
> The configuration console runs on the application server.

To save settings and start the Data Relationship Management service on the application server:

1. In the Configuration Console, click **Save Configuration**.

2. From the **Local Service** menu, click **Start**.

> **⚠ Caution:**
>
> The "Oracle DRM Server Processes" service on all secondary servers **MUST** be started and running **BEFORE** starting the "Oracle DRM Server Processes" service on the application server.

Launching Data Relationship Management in a Web Browser

To launch Oracle Data Relationship Management in a Web browser:

1. Click **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, and then **Web Client**

2. Log in with the ADMIN user ID and password defined during the Repository Wizard process, or an existing user in an upgraded repository.

> **Note:**
>
> If you manually created the repository from scripts, the password is "Welcome!".

Disabling Compatibility View Mode in Internet Explorer

Data Relationship Management does not support Compatibility View mode offered in Microsoft Internet Explorer.

To disable this feature:

1. In Internet Explorer, select **Tools**, and then **Compatibility View Settings**.

2. Make sure that the following options are not selected:

   - Display intranet sites in Compatibility View

   - Display all websites in Compatibility View

3. Click **Close**.

Configuring the Migration Utility

The following table describes Migration Utility configuration settings in the appSettings section of the `web.config` file. This file is located in the following directory by default:
`C:\Oracle\Middleware\EPMSystem11R1\products\DataRelationshipManagement\client\migration-client`

> **Note:**
>
> Any changes made to the `web.config` file will require a restart of the Web site in IIS to take effect.

Table 3-1   Configuration Settings

Key	Description
configuredServers	Specifies the admin-configured connections. Each server connection must be separated by a semi-colon. Syntax is *display*|net.tcp://*URL*/Oracle/Drm/Engine|*name* where: • *display* is the display name • *URL* is the URL for the remote application The URL can be copied from the DRM Console. Select the Host Machines tab and the Engine URL is displayed on the Engine sub tab. • *name* is the user name
showExceptionDetail	Specifies whether detailed exception information is displayed on the error page. **⚠ Caution:** Showing full details may present a security risk, as the detailed information may include file paths or other sensitive information. This setting should only be enabled for debugging or testing. Specify True to enable exception detail or False to display detail according to the log4net settings. The default value is False.
enableAboutPage	Specifies whether the About page is enabled. The About page displays the version of the Migration Utility and system components; for greater security, this page is disabled by default. To check the version of the Migration Utility you can enable this page. To enable the page but restrict access to administrators, edit the Discretionary Access Control List (DACL) on the /Forms/About.aspx file. See the IIS documentation for more information about how DACLs, Directory Security, and anonymous access interact to control access to Web pages. Specify True to show the About page. The default value is False.

Table 3-1   (Cont.) Configuration Settings

Key	Description
HTTPSOnly	Specifies if attempts to connect to this Web application over HTTP protocol are permanently redirected to HTTPS protocol. Specify True to redirect from HTTP protocol to HTTPS. **✎ Note:** The HTTPS protocol must be set up before setting this to True.
XFrameOptionsHeader	Specifies whether the DRM Web application can run in iFrames. Specify SAMEORIGIN to allow the DRM Web application to run inside of a portal using iFrames. Specify DENY to disallow the DRM Web application from running inside of an iFrame. The default setting is DENY.

Increasing Upload File Size

The default limit for uploaded files is 4 MB. To change the default limit to 20 MB, add this setting in the `<system.web>` element of the `web.config` file:

```
<httpRuntime maxRequestLength="20480" executionTimeout="3600" />
```

> **✎ Note:**
>
> By default, the `web.config` file is located in
> `C:\Oracle\Middleware\EPMSystem11R1\products\DataRelationshipManagement\`
> `client\migration-client`.

Load Balancing Data Relationship Management Web Applications

You can configure Oracle HTTP Server to provide load balancing support to two or more Oracle Data Relationship Management Web applications. You set up Oracle HTTP Server to redirect requests to the IIS servers hosting the Data Relationship Management Web client. This procedure assumes that the Oracle HTTP Server installed by the EPM System Installer is the logical host. The EPM System Installer performs the necessary prerequisite checks for

Oracle HTTP Server. For more information, see the *Oracle Enterprise Performance Management System Installation and Configuration Guide* .

To set up Oracle HTTP Server as a load balancer for the Data Relationship Management Web client:

1. Install the Data Relationship Management Web Server component on two or more computers running IIS.

   The Data Relationship Management Installer is generally designed to install the Data Relationship Management client applications to the Default Website, where the Default Website's IIS Site Number is 1. In special circumstances where the first IIS site is non-HTTP, or the Default Website is not IIS Site Number 1, the Data Relationship Management client applications may need to undergo a one-time manual installation into IIS. For any customer impacted with this special situation, contact Support for assistance if needed.

2. Configure Data Relationship Management applications and host computers using the procedure described in Configuring Data Relationship Management Applications.

3. Open the `httpd.conf` file for Oracle HTTP Server found in the following location:

   ```
   MIDDLEWARE_HOME/user_projects/epmsystem1/httpConfig/ohs/config/OHS/
   ohs_component/httpd.conf
   ```

4. Ensure that the following directives exist and are enabled. Add the directives if they do not exist.

   ```
   LoadModule proxy_balancer_module "${ORACLE_HOME}/ohs/modules/
   mod_proxy_balancer.so"
   ```

   ```
   LoadModule headers_module "${ORACLE_HOME}/ohs/modules/mod_headers.so"
   ```

5. Create a proxy balancer definition for the Data Relationship Management Web client by adding a BalanceMember directive for each IIS server that hosts the Data Relationship Management Web Server component.

   ```
   #Configure members for cluster
   <Proxy balancer://iisdrm>
         BalancerMember http://Machine1:80/drm-web-client route=server1
         BalancerMember http://Machine2:80/drm-web-client
   route=server2
   </Proxy>
   ```

6. Enable sticky load balancing by adding the following directives. These sample directives instruct Oracle HTTP Server to insert a cookie that keeps track of the route for sticky load balancing of the proxy balancers defined in the previous step.

   ```
   Header add Set-Cookie "BALANCEID= iisdrm.%{BALANCER_WORKER_ROUTE}e;
   path=/drm-web-client;" env=BALANCER_ROUTE_CHANGED
   ```

7. Add the following Forward and Reverse Proxy directives.

   ```
   #The actual ProxyPass
   ProxyPass /drm-web-client balancer://iisdrm stickysession=BALANCEID
   nofailover=Off
   ```

   ```
   #Do not forget ProxyPassReverse for redirects
   ```

```
ProxyPassReverse /drm-web-client http://<drm_web_server1>:80/drm-web-
client
ProxyPassReverse /drm-web-client http://<drm_web_server2>:80/drm-web-
client
```

8. Save the `httpd.conf` file and restart the Oracle Process Manager server for the Oracle HTTP Server instance.

   After configuration, the Data Relationship Management web application can be accessed using the following URL: `http://<ohs_server>:<port>/drm-web-client`.

Terminating SSL at the Web Server

You can use SSL secure communication from a client's Web browser and the IIS Oracle Data Relationship Management Web application **drm-web-client** using Oracle HTTP Server (OHS). In this configuration, the client's browser communicates with OHS via the HTTPS protocol and OHS acts as a proxy and communicates with the Data Relationship Management Web application via HTTP. See "Terminating SSL at the Web Server" in the *Oracle Enterprise Performance Management System Security Configuration Guide* .

Using Single Sign On with Data Relationship Management

Single Sign On (SSO) for Oracle Data Relationship Management requires various components to be installed and configured. In a typical Web SSO environment, a Web identity management solution controls authentication and authorization for one or more independent software systems. The goal of SSO is to allow a user to gain access to the various independent systems without being prompted for a login for each system.

Data Relationship Management implements SSO by utilizing Oracle Hyperion Shared Services, a web identity management solution (such as Oracle Access Manager), and an external user directory (such as Oracle Internet Directory or Microsoft Active Directory).

> **Note:**
>
> A mix of SSO and non-SSO applications is not supported on a single server.

Use the following steps to install and configure SSO:

Task	Reference
Prerequisite	
Install and configure Oracle Access Manager 12c	See *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* and *Fusion Middleware Administrator's Guide for Oracle Access Management*
Data Relationship Management	
1. Configure Shared Services with an external user directory.	See "Configuring OID, Active Directory, and other LDAP-based User Directories" in the *Oracle Enterprise Performance Management System User Security Administration Guide* .

Task	Reference
2. Configure Shared Services for SSO.	See "Configuring EPM System for SSO" in the *Oracle Enterprise Performance Management System Security Configuration Guide* .
3. Install Data Relationship Management.	See Installing Data Relationship Management.
4. In the Data Relationship Management Configuration Console, configure Data Relationship Management for CSS authentication mode and enable SSO.	See Configuring Host Computers.
5. Configure a Web identity management solution to protect the Data Relationship Management Web application and use the same external user directories configured in Shared Services.	See Web Access Management.
6. Install and configure IIS OAM Webgate	*Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*
Data Relationship Management Analytics	
1. Ensure that the Oracle EPM Foundation Server has been configured with Oracle HTTP Server. This can be accomplished by configuring the Web Server in the EPM System Configurator.	
2. Manually configure the following directive in the file `mod_wl_ohs.conf` (assuming default port of 9800 for the DRMServer managed server and replacing HOST with the host name). File can be found at : `<MW_HOME>\user_projects\epmsystem1\httpConfig\ohs\config\OHS\ohs_component` `<LocationMatch^/oracle-epm-drm-analytics>` `SetHandler weblogic-handler WeblogicHost HOST WeblogicPort 9800 WLIOTimeoutSecs 6000 Idempotent OFF WLSocketTimeoutSecs 600` `</LocationMatch>`	
3. Install 11.1.2.2 Webgate for OHS	See "Installing Oracle HTTP Server 11g Webgate" in *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*
4. Deploy and configure webgate instance using tool deployWebGate	See "Post-Installation Steps for Oracle HTTP Server 11g Webgate" in *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*
5. Register Webgate	See "Getting started with a New Oracle HTTP Server 11g Webgate" in *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*
6. Configure the OAM Identity Asserter	See "Configuring the OAM Identity Asserter" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*
7. Configure external authentication provider for WebLogic domain	See "Configuring LDAP Authentication Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server 10.3.6*

Task	Reference
8. Configure the default authenticator	See "Configuring the Default Authenticator and Provider Order" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*
9. Restart Weblogic Admin and DRM Managed Servers	
10. Restart Oracle Process Manager (Oracle HTTP Server)	

Web Access Management

The Oracle Data Relationship Management Web application resources must be protected so that any request to the Web application is redirected to a Web access management application, such as Oracle Access Manager. After a user authenticates with the security agent using basic authentication, the agent forwards the request to the Data Relationship Management Web application where HTTP header information is passed to the Data Relationship Management server for authentication.

Oracle Access Manager

Oracle Access Manager (OAM) provides authentication and authorization for the Oracle Data Relationship Management Web applications. In this documentation, it is assumed that OAM has been installed and configured with access policies for the Data Relationship Management Web application. For more information, see "Managing Policies to Protect Resources and Enable SSO" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

Data Relationship Management can be configured with Oracle Access Manager using one of the following options:

- Install and configure Oracle Access Manager 10g or 11g Webgate for IIS on the Data Relationship Management Web server. For the Oracle Access Manager 10g Webgate for IIS download, see the Readme file for "Oracle Access Manager 10g – non OHS 11g Webgates and 3rd Party Integrations".

    > **Note:**
    >
    > Oracle Access Manager Patch 20216345 is required. For more information, go to Oracle Support.

- Set up Oracle HTTP Server for load balancing the Data Relationship Management Web server and install Oracle Access Manager 11g Webgate for OHS. See "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM " in *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

Oracle Data Relationship Management Analytics can be configured with Oracle Access Manager by installing and configuring Oracle Access Manager 11g webgate for OHS. See "Installing and Configuring Oracle HTTP Server 11g WebGate for OAM" in *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*.

The WebGate module intercepts HTTP requests for Web content on the web server and forwards the requests to Oracle Access Manager.

The following graphic depicts the process flow with Oracle Access Manager using the 10g Webgate for IIS on the Data Relationship Management Web server:

4
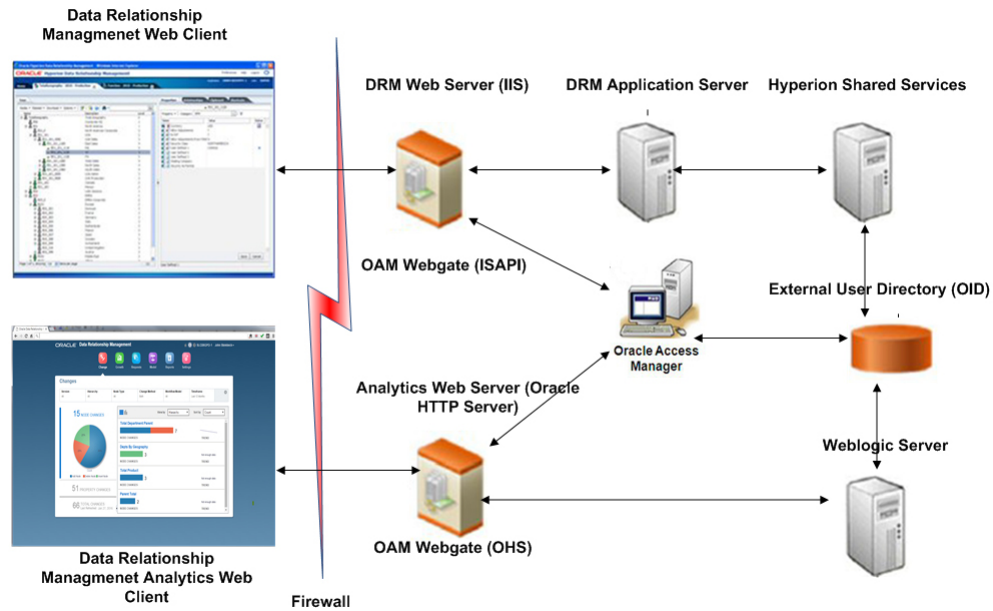
Deploying and Configuring the Data Relationship Management Web Services API

The Oracle Data Relationship Management Enterprise Archive Application (oracle-epm-drm-webservices.ear) includes Web service modules that provide integration with the Data Relationship Management server. The application archive contains the DrmService and DrmGovernanceService Web services modules which can be accessed over HTTP using the SOAP protocol. The Web services are implemented in Java and are deployed to the WebLogic application server. Both services communicate internally with the Data Relationship Management API Adapter service.

The Web services require users to be authenticated using an external user directory which is accessible by both Weblogic and Oracle Hyperion Shared Services.

Before deploying the Data Relationship Management Web Service API, review Figure 3.

System Requirements

- Oracle WebLogic Server 12c

- Oracle Data Relationship Management API Adapter

- Oracle Web Services Manager (OWSM)

- Oracle Hyperion Shared Services

- An external user directory such as Oracle Internet Directory or Microsoft Active Directory

> **Note:**
>
> For the latest requirements, see the *Oracle Enterprise Performance Management System Certification Matrix* posted on the Supported System Configurations page on Oracle Technology Network (OTN):
>
> https://www.oracle.com/middleware/technologies/bi-foundation/hyperion-supported-platforms.html

Deployment Prerequisites

Installing and Configuring Foundation Services

To support HTTP Basic Authentication and Web Services (WS) Security for the Oracle Data Relationship Management Web Service applications, Oracle Hyperion Foundation Services must be installed and Data Relationship Management must be configured to use Oracle Hyperion Shared Services for authentication. Oracle Web Services Manager (OWSM) is required for the oracle-epm-drm-webservice application but is not required for the oracle-

epm-drg-rest-webservice application. OWSM is installed when you install Foundation Services but it may need to be configured if it hasn't already been done. For information on installing Foundation Services, see *Oracle Enterprise Performance Management System Installation and Configuration Guide* .

Installing Metadata Services Schema for Oracle Web Services Manager

Oracle Web Services Manager requires a database in order to function. Requirements and instructions on how to install the Metadata Services Schema for Oracle Web Services Manager can be found here:

- "Creating Infrastructure Schemas Using Repository Creation Utility" in *Oracle Enterprise Performance Management Installation and Configuration Guide*

- "Repository Creation Utility (RCU) Requirements" in *Oracle Fusion Middleware System Requirements and Specifications*

> **Note:**
>
> Oracle Fusion Middleware documentation is available at http://www.oracle.com/technetwork/indexes/documentation/index.html#middleware.

Configuring Oracle Web Services Manager

To configure Oracle Web Services Manager, refer to "Configuring Oracle Web Services Manager" in the *Oracle Enterprise Performance Management System Deployment Options Guide* .

Configuring WebLogic with an External Provider

The Oracle Data Relationship Management Web Service application deployed on Weblogic must be configured to access the same user directory that is configured with Oracle Hyperion Shared Services for externally authenticating users.

To configure WebLogic, see "Configuring the WebLogic Domain to OID, MSAD, SunOne" in the *Oracle Enterprise Performance Management System Deployment Options Guide* .

Configuring the API Adapter

The API Adapter must be configured using the Oracle Data Relationship Management Configuration Console. When you configure a Data Relationship Management application, you set up API Adapter Hosts on the Host Machines tab. For more information, see Configuring Host Computers.

> **Note:**
>
> The API Adapter is used for internal communication with the Web Service and should not be used directly by custom API programs.

Deploying the Web Services Applications

The Oracle Data Relationship Management Web service applications `oracle-epm-drm-webservices.ear` and `oracle-epm-drm-rest-webservices.ear` should be deployed to an existing WebLogic domain and managed server. For example, the Web services can be deployed to the EPMServer0 managed server on the EPMSystem domain within the EPM Foundation Server. Both `.ear` files are located in the `%EPM_ORACLE_HOME%\products\DataRelationshipManagement\api` directory of the application server machine.

Instructions for installing a Web application can be found in Deploying Web Services Applications in *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

> **Note:**
>
> Oracle Fusion Middleware documentation is available at http://www.oracle.com/technetwork/indexes/documentation/index.html#middleware.

Securing the Data Relationship Management Web Services

It is important to protect the DrmService and DrmGovernanceService Web services using a security policy in Oracle Web Services Manager. Different policies may be attached depending on usage.

The following policies can be used with the Oracle Data Relationship Management Web services:

Purpose	Policy
Integration with Oracle Hyperion Financial Data Quality Management, Enterprise Edition	oracle/wss_username_token_service_policy or oracle/wss_username_token_service_policy (applies to DrmService only)
Integration with E-Business Suite General Ledger	oracle/wss_username_token_service_policy (applies to DrmService only)
Integration with Oracle Fusion Accounting Hub	oracle/wss_saml_or_username_token_service_policy (applies to DrmService only)
Workflow Development Kit	oracle/wss11_saml_or_username_token_with_message_protection (applies to DrmService only)

Purpose	Policy
Custom API Programs or Integrations	One of the following (applies to DRMService and DRMGovernanceService): • oracle/wss11_saml_or_username_token_with_message_protection • oracle/wss_username_token_service_policy • oracle/wss_saml_or_username_token_service_policy • oracle/wss_http_token_service_policy

See "Attaching Policies to Web Services" in *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

Configuring Policies in Oracle Web Services Manager

To configure policies for the DrmService and DrmGovernanceService modules in Oracle Web Services Manager, see "Configuring Policies" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

When configuring a web service security policy that uses message protection, a keystore must be configured to be used for encryption purposes. To configure a keystore, refer to "Setting Up the Keystore for Message Protection" in the *Oracle Enterprise Performance Management System Deployment Options Guide* .

Testing the Data Relationship Management Web Services Using Oracle Enterprise Manager

To test the Web Services using Oracle Enterprise Manager:

1. Ensure that the Oracle Data Relationship Management Web Service has an Oracle Web Services Manager security policy attached. A local or global policy can be attached.

   For example: `oracle/wss_username_token_service_policy`

   > **Note:**
   >
   > You can have only one policy at a time attached to the Data Relationship Management Web Service. After changing the security policy, you may need to restart the WebLogic target server to which the Data Relationship Management Web Service is deployed.

2. In Enterprise Manager, select the domain to which the Data Relationship Management Web Service is deployed, then select **Web Services/Test Web Service** from the domain context menu or the **WebLogic Domain** menu in the right pane. .

3. Enter the WSDL for the Data Relationship Management Web Service in the WSDL text box.

For example: `http://localhost:28080/oracle-epm-drm-webservices/DrmService?wsdl`

4. From **Operation**, select an operation; for example getSysPrefs.

5. On the **Request** tab, select **WSS Username Token** and enter a username and password with which to authenticate.

> **Note:**
>
> The user must exist in the security realm for the WebLogic domain and in Oracle Hyperion Shared Services.

6. Expand **Input Arguments**, from the drop-down list select **XML View**, and paste the following soap header argument (exactly as formatted) before the "`<soap:Body xmlns:ns1="http://drm.webservices.epm.oracle">`" tag.

   When copying the argument below, there cannot be a line break or space between tags/elements.

```
<soap:Header>
<AppParameters xmlns="http://drm.webservices.epm.oracle">
<serverUrl xmlns="http://drm.webservices.epm.oracle">http://
localhost:5240/Oracle/Drm/APIAdapter</serverUrl>
<sessionParams xmlns="http://
drm.webservices.epm.oracle">ProductVersion=11.2.0,CultureName=en-
US,UICultureName=en-US, TimeZoneID=Eastern Standard Time</sessionParams>
</AppParameters>
</soap:Header>
```

   Considerations

   • An AppParameters element must occur in the header for the message to process correctly at the Data Relationship Management and Oracle Data Relationship Governance Web services.

   • When using Stateful Sessions in the Data Relationship Management and Data Relationship Governance Web services, the SessionMaintainParams element must occur before the AppParameters element in the SOAP header, otherwise, the Stateful Session ID will not be recognized and will not be processed.

   • Required parameters must be populated for the selected Data Relationship Management operations otherwise an error occurs.

7. In the soap header argument in step 6, modify the `serverUrl` to the appropriate host name and port for the Data Relationship Management API adapter.

8. Click **Test Web Service**.

> **Note:**
>
> If successful, the **Response** tab includes the response from the Web Service. If unsuccessful, an error message is displayed.

9. After testing is complete, re-attach the required production policy.

Configuring Logging for the Web Service Applications

Optionally, Oracle Diagnostics Logging (ODL) can be configured to log specific logging levels to a log file that is specific for one or more logger names. To configure logging, the Weblogic Scripting Tool (WLST) can configure the logger names specific to the Oracle Data Relationship Management Web services:

- oracle.epm.drg
- oracle.epm.drm
- oracle.epm.webservices.drm
- oracle.epm.webservices.drg

See setLogLevel and configureLogHandler commands in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Troubleshooting

Error	Possible Cause	Recommendation
Oracle EPM Foundation Agent Error in request: begin session (message: Cannot begin session. EPMCSS-00301: Failed to authenticate user. Invalid credentials. Enter valid credentials.	Oracle Hyperion Shared Services doesn't contain the user identity.	Ensure Oracle Data Relationship Management is configured with the same User directory as used by the WebLogic realm.
javax.xml.ws.soap.SOAPFaultException: FailedAuthentication : The security token cannot be authenticated.	User identity is not present in WebLogic security realm.	Configure the WebLogic Realm with the appropriate authentication provider for the realm. Ensure that it is configured to point to the same provider with which Shared Services is configured.
javax.xml.ws.WebServiceException: Failed to access the WSDL at: http://localhost:7001/oracle-epm-drm-webservices/DrmService?WSDL.	Host or port is incorrect. The Web service is not running on the WebLogic domain.	Verify the Data Relationship Management Web service is deployed and running on the WebLogic domain. Modify the host/port reference in the WSDL URL.
Error while trying to communicate with DRM API Adapter at: http://localhost:5240/Oracle/Drm/APIAdapter/.	Host or port is incorrect. The API adapter is not running or configured correctly.	Verify the API adapter is configured and running. Change the API adapter URL in the client program/application to the correct value.

Error	Possible Cause	Recommendation
javax.xml.ws.soap.SOAPFaultException: SOAP must understand error: {http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd}Security, {http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd}Security.	No OWSM policy is attached to the Data Relationship Management Web service or, if a policy exists, the policy is disabled. OWSM is not configured correctly and is not functioning. Ensure that the servlet can be reached and that the Policy Manager Status is "Operational" http://\<host\>:\<port\>/wsm-pm/validator	Attach either a global or local policy to the Data Relationship Management Web service. Follow the steps in the OWSM troubleshooting section: http://download.oracle.com/docs/cd/E12839_01/web.1111/b32511/diagnosing.htm#CHDIDCHA

5
Installing and Configuring Data Relationship Management Analytics

The Oracle Data Relationship Management Analytics module provides dashboards for change tracking, growth analysis, request monitoring, workflow model performance, and participant and user group performance. The module supports Single Sign On and provides the ability to drill to and from Oracle Data Relationship Management.

System Requirements

- Oracle Database—Set open_cursors to a value greater than or equal to 600 for the database hosting the Oracle Data Relationship Management application schema.

  > **Note:**
  >
  > SQL Server is not supported.

- EPM Foundation Server

  > **Note:**
  >
  > For LDAP instructions see "Configuration OID, Active Directory and other LDAP-based user directories" in *Oracle Enterprise Performance Management System Security Configuration Guide* .

- Data Relationship Management

  – Application schema hosted on Oracle database

  – EPM Foundation installed with Data Relationship Management on compatible releases for Data Relationship Management External Authentication of Analytics users. See the Release Compatibility tab of the the *Oracle Enterprise Performance Management System Certification Matrix* posted on the Supported System Configurations page on Oracle Technology Network (OTN):)

    https://www.oracle.com/middleware/technologies/bi-foundation/hyperion-supported-platforms.html

  – Oracle Data Relationship Management Analytics users must be defined in an External Directory available for user authentication in both WebLogic and Oracle Hyperion Shared Services

- EPM System—A configured EPM Instance, on the same release level with Data Relationship Management, where the "DRMServer" WL Managed Server can be created for Analytics deployment in either a Windows or Linux WL Domain configured within the EPM Instance.

> **Note:**
>
> For Data Relationship Management Analytics deployments, the default name of the WebLogic domain is EPMSystem and is hardcoded into the `createDrmSvc.cmd` file. If your domain is not named EPMSystem then, before running an installation or upgrade, you must edit the `createDrmSvc.cmd` file to change EPMSystem to the name of your domain. Edit the following lines in the `createDrmSvc.cmd` file.
>
> ```
> set USERDOMAIN_HOME=%MW_HOME%\user_projects\domains\EPMSystem
>
> call"%MW_HOME%
> \user_projects\domains\EPMSystem\bin\setDomainEnv.cmd"
> ```

- Hardware—The DRMServer that will be created requires at least 4096 MB of RAM in a production environment.

> **Note:**
>
> The Windows file `startDRMServer.cmd`, the Windows Service "Oracle DRM Managed Server (DRMServer)," and the Linux file `startStopDRMServer.sh` set memory to 4096 MB by default. When sizing hardware, these settings, as well as the minimum required memory for non-production environments, should be considered.

- If you are configuring Data Relationship Management and Data Relationship Management Analytics for Single Sign On, see Using Single Sign On with Data Relationship Management .

Deployment Prerequisites

If you are configuring Oracle Data Relationship Management and Oracle Data Relationship Management Analytics for single sign on, also see Using Single Sign On with Data Relationship Management .

> **Note:**
>
> Only one copy of Data Relationship Management Analytics can be deployed, and it can only start up and run against a single Data Relationship Management application.
>
> The only supported way to deploy more than one copy of Data Relationship Management Analytics is if you are running the EPM Instance on both Windows and Linux. In this scenario, each operating system has its own WebLogic domain and one copy of Data Relationship Management Analytics can be deployed per WebLogic domain, supporting up to a total of two distinct Data Relationship Management applications.

In the Data Relationship Management Console, select the application configure the following:

- Use the Repository Wizard to configure the Data Relationship Management schema—See Creating a Repository

- Set authentication mode to Mixed or CSS–See Configuring Authentication Settings.

- Enable the CSS Bridge–See Configuring the CSS Bridge

- Configure Web Farm settings to enable drill through between Data Relationship Management and Data Relationship Management Analytics—See Configuring Web Servers

- Configure the Analytics URL settings to enable drill through between Data Relationship Management and Data Relationship Management Analytics—Configuring Analytics URL

- Data Relationship Management Analytics users must be defined in an External Directory that is configured for user authentication in both WebLogic and Oracle Hyperion Shared Services

Installing and Configuring Data Relationship Management Analytics

> ⚠️ **Caution:**
>
> Make sure that EPMServer and Weblogic AdminServer are shut down before starting the installation.

> ✎ **Note:**
>
> The installation script for Windows is `installConfigureAnalytics.cmd`. The installation script for Linux is `installConfigureAnalytics.sh`.

To install Oracle Data Relationship Management Analytics:

1. Download the Analytics zip file to the server where Oracle EPM Foundation Server is installed.

2. Unzip the file into a temporary folder.

3. Run the script `installConfigureAnalytics.*` to install the Analytics package and initiate the Fusion Middleware Configuration Wizard to configure and deploy the Analytics application. When prompted, enter the following information in the scripting console.

   > ✎ **Note:**
   >
   > Linux users complete the first 2 steps only. Windows users complete all steps.

   a. Oracle Middleware Home directory and then press Enter.

    b. EPM Domain name and press Enter.

    For Linux only, the Fusion Middleware Configuration Wizard will start.

    c. Weblogic administrator username and then press Enter.

    d. Weblogic administrator password and then press Enter.

    e. AdminServer Host name and then press Enter.

    f. AdminServer Port and then press Enter.

    For Windows only, the Fusion Middleware Configuration Wizard will start.

4. In the Fusion Middleware Configuration Wizard, select **Extend an existing WebLogic domain** and then click **Next**.

5. Select the domain directory for the target WebLogic domain within the EPM Instance (Windows or Linux) for DRMServer and then click **Next**.

6. Under **Extend my domain automatically to support the following added products** select **Oracle Data Relationship Management Analytics - 11.1.2.4 [EPMSystem11R1]** and then click **Next**.

7. Click **Next** on the **Configure EPMSystemRegistry JDBC Data Sources** screen to skip the configuration.

8. Click **Next** on the **Test EPMSystemRegistry JDBC Data Sources** screen to skip testing.

9. Enter the following on the **Configure JDBC Component Schema** screen for the DRM Schema and then click **Next**:

- Schema Owner
- Schema Pasword
- DBMS/Service
- Host Name
- Port

10. On the **Test JDBC Component Schema** screen, ensure that the test is successful for the DRM Schema.

11. On the **Select Optional Configuration** page, select both check boxes: **Select Managed Servers, Clusters and Machines** and **Deployments and Services** and then click **Next**.

12. On the **Configure Managed Servers** screen, view the DRMServer, change the port if necessary, and then click **Next**.

13. Click **Next** on the **Configure Clusters** screen to skip.

> **✐ Note:**
>
> Do not move the DRMServer under the existing EPMServer or FoundationServer depending on configuration.

14. On the **Assign to Clusters** screen click **Next** and accept the defaults on the next few screens until you get to the **Assign Servers to Machines** screen.

15. On the **Assign Server to Machines** screen, select the DRMServer and move it under the appropriate machine.

16. On the **Target Deployments to Clusters or Servers** screen, ensure that the **oracle-epm-drm-web-applications** application is set only on the target DRMServer and then click **Next**.

> **Note:**
>
> To verify, click on the Cluster and Server nodes on the left target pane to see if the **oracle-epm-drm-web-applications** deployment is selected for the DRMServer.

17. On the **Target Services to Clusters or Servers** screen, ensure that the **DRM** JDBC Datasource is only targeted to the DRMServer and then click **Next**.

> **Note:**
>
> To verify, click on the Cluster and Server nodes on the left target pane to see if the DRM data source is selected only for the DRMServer.

18. Click **Extend** on the **Configuration Summary** screen, and when complete click **Done** to exit the wizard.

19. Start AdminServer.

AdminServer can be started on Windows by running the command file, for example `C:\Oracle\Middleware\user_projects\domains\EPMSystem\bin\startWebLogic.*`.

> **Note:**
>
> Ensure AdminServer has completely started before starting the DRMServer.

20. Start DRMServer.

- Windows Only—DRMServer Managed Server can be started by starting the Windows Service "Oracle DRM Managed Server (DRMServer)" or by using the `startDRMServer.cmd` file.

  > **Note:**
  >
  > It is recommended that you use the Windows Service if you are running the Managed Server in the background.

- Linux Only —DRMServer Managed Server can be started by using the `startStopDRMServer.sh` script in the domain bin folder. For example:

  `<MiddlewareHome>\user_projects\domains\EPMSystem\bin\startStopDRMServer.sh`

To start the DRMServer, issue the following command:
`startStopDRMServer.sh start`. To stop the DRMServer, issue the following command: `startStopDRMServer.sh stop`.

> **Note:**
>
> During the initial installation, ensure that the AdminServer has completely started before attempting to start the DRMServer Managed Server.

21. Configure Weblogic Security Provider. See "Configuring WebLogic Security Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server 10.3.6*.

> **Note:**
>
> Ensure that you configure the same external directory that is configured for the EPM Foundation Server.

Upgrading Data Relationship Management Analytics

> ⚠ **Caution:**
>
> The AdminServer and DRMServer should not be running when performing the upgrade.

To update an existing Oracle Data Relationship Management Analytics application:

1. Obtain the updated Analytics zip file.
2. Unzip the zip file.
3. For Linux, complete steps 4-6. For Windows, complete steps 4-10
4. Run the script `upgrade.*` in the upgrade folder to initiate an upgrade.
5. Enter Oracle Middleware Home directory and then press Enter.
6. Enter the EPM Domain name and then press Enter.

   For Linux only, the upgrade is complete and you are prompted to restart DRMServer.
7. Enter the Weblogic administrator username and then press Enter.
8. Enter the Weblogic administrator password and then press Enter.
9. Enter the AdminServer Host name and then press Enter.
10. Enter the AdminServer Port and then press Enter.

    For Windows only, the upgrade is complete and you are prompted to restart DRMServer.

Logging

A persistent ODL logger is automatically configured for the Oracle Data Relationship Management Analytics application. Manual configuration of the managed server is not necessary. However, by default the logger level is set to the NOTIFICATION:1 level. If tracing is desired then set the level to TRACE:1 by navigating to Enterprise Manager and turning on debugging levels using the Configure Logging menu for the application.

Troubleshooting

When importing (impdp) an Oracle dump file for a Oracle Data Relationship Management Analytics schema to an Oracle database instance where another Data Relationship Management Analytics schema already exists, the following error may occur:

Example 5-1   Error

```
ORA-39083: Object type TYPE failed to create with error:
ORA-02304: invalid object identifier literal
Failing sql is: CREATE TYPE "<schemaName>"."FILTERVALUES_TABLE_TYPE"  OID
'BD565ED4E40844C69873A972C29FE5A9' as TABLE of varchar2 (255)
```

The error occurs if the dump file includes the Data Relationship Management Analytics 'TYPE' object with a specific Oracle identifier (OID). As a result of the error condition, the imported Data Relationship Management Analytics schema will not function properly.

Workaround

To resolve the error during import, include parameter/value "TRANSFORM=oid:n" in the Data Pump Import command or script. Refer to Oracle Database documentation for details on the Data Pump Import TRANSFORM parameter.

6

Upgrading a Data Relationship Management Installation

Upgrading is the process of deploying a new software release and moving applications and data from the earlier deployment to the new deployment.

The main initial certification of Oracle Enterprise Performance Management System products per the 11.2 certification matrix is described below.

Product	Certification
Application operating system	Windows 2019
Oracle database	Oracle 12c (12.2.0.1+)
Microsoft SQL database	Microsoft SQL Server 2016
JDK	Oracle JDK 1.8.0_131+

Supported Upgrade Paths

Oracle Data Relationship Management Release 11.2.0 is a platform release so there is no strict upgrade of the application from previous releases. It is certified to be deployed on a Windows 2019 operating system. Install Data Relationship Management Release 11.2 on a Windows 2019 OS that has not had Data Relationship Management previously installed on it.

To migrate a previous repository, start with a repository that has been staged on Data Relationship Management 11.1.2.4.xxx. If the repository is currently on a Data Relationship Management release earlier than 11.1.2.4.xxx, upgrade that repository to 11.1.2.4.xxx first and validate that the upgrade was successful.

Follow the steps below:

1. Stop the Data Relationship Management application and exit the Data Relationship Management Configuration Console.

2. Migrate repository:

    a. For an Oracle db Repository, use the database EXPDP process to export the repository schema for each application and stage in a new schema on an Oracle 12c (12.2.0.1+) database using the IMPDP utility.

    b. For MSSQL Server, use the SQL Server management tools to create a backup of the database and restore it to a new MSSQL 2016 database.

3. Start the Data Relationship Management Configuration Console and create an application for each repository intended to be migrated, filling in the configuration information as appropriate to point to the repository backup staged on an Oracle 12c (12.2.0.1+ database server) or MSSQL 2016 server.

4. Run **Apply Updates** on the application.

Upgrading Checklist

The following table identifies the high-level tasks that you perform to upgrade Oracle Data Relationship Management.

Table 6-1   Upgrading Checklist

Task	Reference
1. Review release compatibility, system requirements, and other prerequisites for this release. If your database environment needs to be upgraded, perform the database upgrade before you proceed. See the database documentation for details. **Note:** If you are using Oracle Hyperion Shared Services, you must upgrade the Shared Services installation before upgrading the Data Relationship Management. For more information, see the *Oracle Enterprise Performance Management System Installation and Configuration Guide* .	• Installation Prerequisites • *Oracle Enterprise Performance Management System Certification Matrix* posted on the Supported System Configurations page on Oracle Technology Network (OTN): https://www.oracle.com/middleware/technologies/bi-foundation/hyperion-supported-platforms.html • *Oracle Enterprise Performance Management System Installation and Configuration Guide*
2. Back up the earlier release.	Before you proceed with an upgrade, ensure that you have backed up information from the earlier release including databases, applications, and other files. Back up the `drm-config.xml` file before upgrading. This file is not backward compatible with earlier releases.
3. Download and prepare the installation files.	Download files for this release and extract the zip file contents.
4. Stop Data Relationship Management services.	If you are installing this release on the same machine as the earlier release installation, stop the Data Relationship Management services.
5. Uninstall the earlier release of Data Relationship Management.	If you are upgrading, you must first manually uninstall the old release and then install the new release.
6. Install this release of Data Relationship Management	Installing Data Relationship Management.
7. Configure Data Relationship Management.	Use the Data Relationship Management Configuration Console to configure the new installation.
8. Redeploy the Web Service for this Data Relationship Management release. **Note:** If upgrading the Web service from a release prior to 11.1.2.1, the Web service DrmWebService must be undeployed using the WebLogic console. Instructions on how to undeploy a Web service can be found in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services.*	The name of the Web service application in WebLogic is "oracle-epm-drm-webservices" by default.

Table 6-1   (Cont.) Upgrading Checklist

Task	Reference
9. Optional: Deploy and configure the Web Service.	Deploying and Configuring the Data Relationship Management Web Service API
10. Start Data Relationship Management services.	

Applying Updates to an Application

To apply updates to an existing 11.1.2.x repository:

1. Create a new application.

2. On the **Repository Configuration** tab, specify repository connection information for an existing 11.1.2.x repository.

3. Select the application from the **Applications** list.

4. From the **Application** menu, select **Apply Updates**.

> ✎ **Note:**
>
> The **Apply Updates** option is not applicable to any release prior to 11.1.2.0.x.

Manual Upgrade Tasks

Related Topics

• Upgrading Properties with Derived Property References

• Upgrading Batch Client Scripts

• Upgrading API Programs

Upgrading Properties with Derived Property References

For derived property formulas from a pre-11.1.2.1 application that reference a calculated property name based on the value of other properties at run time, the formulas must be manually edited to insert the namespace prefix (Custom or Core) using the Concat function. The application upgrade process cannot identify or automatically convert derived properties of this nature since the referenced property names are only calculated during the evaluation of the formula for a node.

For example, a formula which derives the value of the property returned from the MyPropName property before upgrade:

```
PropValue(PropValue(MyPropName))
```

The explicit property reference is updated to Custom.MyPropName after upgrade:

```
PropValue(PropValue(Custom.MyPropName))
```

However, the value returned from the Custom.MyPropName property at runtime also needs to be identified in a particular namespace. The formula needs to be manually edited to concatenate the appropriate namespace in order for the outer PropValue function to evaluate correctly:

```
PropValue(Concat(Custom.,PropValue(Custom.MyPropName)))
```

Upgrading Batch Client Scripts

To function properly, you must manually upgrade Batch Client scripts from releases before 11.1.2 by making these changes:

- Change the Batch Client program name to `drm-batch-client.exe`

- Change the URL to the Oracle Data Relationship Management application (refer to the Process Manager URL on the Host Machines tab of the Configuration Console).

See the *Oracle Data Relationship Management User's Guide* for information on Batch Client parameters.

Upgrading API Programs

API programs using the 11.1.2.4 Web service API can be manually upgraded to work with the Web service API in this release. To manually upgrade, you must regenerate proxy classes, rebuild projects, and resolve build errors that may arise from changes to previously used methods and types. See Oracle Data Relationship Management API Guide for instructions on using the Web service API and regenerating Web service proxy classes.

API programs used with Oracle Data Relationship Management releases prior to 11.2 must be manually modified to use the Web service API offered in this release.

Troubleshooting

Error	Cause	Workaround
DRM-61043: The following error occurred registering the application with HSS: Can't find 'com/oracle/drm/EpmRegistryclient'	In Oracle Data Relationship Management 11.1.2.2, the JAR ..\DataRelationshipManagement\server\jar\drm-epm-registry.jar was not part of the release. This was added later to provide expanded EPM Registry integration. In Data Relationship Management 11.1.2.4.x, this entry must exist in the Class Path list below the CSS Tab in the Data Relationship Management Console, and the upgrade will not auto-insert that Class Path line into the Data Relationship Management Config XML file.	Add the additional Class Path manually to the 11.1.2.4.x config in the Data Relationship Management Console. You must restart Data Relationship Management to propagate the Class Path update completely. Restarting the Data Relationship Management Console executable alone is not sufficient for the change to take effect.

7

Monitoring Data Relationship Management Applications

Oracle Data Relationship Management applications can be monitored using the Configuration Console.

Application Status

Application status information is located on the following tabs:

- **Running Processes** – You can view the computer name, name and port number of each process, the start time of the process, and memory and CPU usage for the process.

- **Loaded Versions** – You can view the name of each version, the computer name, and the engine for each version.

- **Current Sessions** – You can view the user names logged into the application, including the time of login and the time of last activity.

To view application status information:

1. Open the Oracle Data Relationship Management Configuration Console by selecting **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, and then **Configuration Console**.

2. Select an application and then click **Application Status**. Use the tabs noted above to view information for the application.

Computer Status

Computer status information is located on the following tabs:

- **Machine Information** – You can view the computer name, operating system, version, time the computer started running, and the Oracle Data Relationship Management Windows account.

- **Running Processes** – You can view the name and port number of each process, the start time of the process, and memory and CPU usage for the process.

- **Windows Event Log** – You can view recent events, such as warnings, the source of the event, and the event message.

To view computer status information:

1. Open the Data Relationship Management Configuration Console by selecting **Start**, then **Programs**, then **Oracle EPM System**, then **Data Relationship Management**, and then **Configuration Console**.

2. Expand an application and select the computer name. Use the tabs noted above to view information for the computer.