Oracle® Data Relationship Management

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

Installation Guide
Release 11.1.2.3.500
Updated: November 2014
Contents

Documentation Accessibility ........................................................... 7

Documentation Feedback ............................................................. 9

Chapter 1. Installing Data Relationship Management ......................................... 11
   Installation Prerequisites .................................................................. 11
       Architecture Options ................................................................... 12
       64-bit Operating System ............................................................ 17
       Windows Server 2008 Prerequisites .......................................... 17
       Oracle Database Prerequisites .................................................. 18
       SQL Server Database Prerequisites ......................................... 19
       PDF Font Requirement for Asian Glyphs .................................... 19
       Virtual Memory Pagefile Sizing ................................................ 19
   Additional Documentation ................................................................ 19
   About Middleware Home and EPM Oracle Home .............................. 20
   Foundation Services ...................................................................... 20
       Data Relationship Management CSS Bridge ............................... 21
       Deployment Scenarios for Data Relationship Management and Foundation Services ......................................................... 21
   Installing Data Relationship Management ................................... 22
   Installing Data Relationship Management in a Distributed Environment ......... 23
   Installing Secondary Engine Hosts .............................................. 23
   Installing Secondary Data Relationship Management Web Server Hosts .......... 24
   Installing Secondary API Adapter Hosts ....................................... 24
   Installing Secondary Foundation Services Hosts ............................ 24
   Troubleshooting ........................................................................ 24

Chapter 2. Configuring Data Relationship Management .................................. 25
   Configuring Foundation Services for Data Relationship Management .......... 25
   Configuring Secondary Foundation Services Hosts .......................... 26
   Configuring Shared Services with an External Provider .......................... 27
   Configuring Shared Services for Single Sign On .................................. 27
   Configuring CSS Mode for Data Relationship Management ................ 27
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting the Data Relationship Management Configuration Console</td>
<td>27</td>
</tr>
<tr>
<td>Configuring Data Relationship Management Applications</td>
<td>27</td>
</tr>
<tr>
<td>Creating an Application</td>
<td>28</td>
</tr>
<tr>
<td>Application Controller</td>
<td>28</td>
</tr>
<tr>
<td>Setting the Application Default Culture</td>
<td>29</td>
</tr>
<tr>
<td>Date, Time, and Number Formatting</td>
<td>29</td>
</tr>
<tr>
<td>Creating a Repository</td>
<td>30</td>
</tr>
<tr>
<td>Copying a Repository</td>
<td>34</td>
</tr>
<tr>
<td>Configuring Host Computers</td>
<td>34</td>
</tr>
<tr>
<td>Configuring Authentication Settings</td>
<td>38</td>
</tr>
<tr>
<td>Configuring EPM Registry Settings</td>
<td>39</td>
</tr>
<tr>
<td>Configuring Scheduled Tasks</td>
<td>40</td>
</tr>
<tr>
<td>Removing an Application</td>
<td>41</td>
</tr>
<tr>
<td>Saving Configuration Settings and Starting the Service</td>
<td>41</td>
</tr>
<tr>
<td>Launching Data Relationship Management in a Web Browser</td>
<td>41</td>
</tr>
<tr>
<td>Disabling Compatibility View Mode in Internet Explorer</td>
<td>41</td>
</tr>
<tr>
<td>Configuring the Migration Utility</td>
<td>42</td>
</tr>
<tr>
<td>Increasing Upload File Size</td>
<td>42</td>
</tr>
<tr>
<td>Load Balancing Data Relationship Management Web Applications</td>
<td>43</td>
</tr>
<tr>
<td>Terminating SSL at the Web Server</td>
<td>44</td>
</tr>
<tr>
<td>Using Single Sign On with Data Relationship Management</td>
<td>44</td>
</tr>
<tr>
<td>Web Access Management</td>
<td>45</td>
</tr>
<tr>
<td>Configuring Web Client Help</td>
<td>46</td>
</tr>
<tr>
<td>Chapter 3. Deploying and Configuring the Data Relationship Management Web Service API</td>
<td>49</td>
</tr>
<tr>
<td>System Requirements</td>
<td>49</td>
</tr>
<tr>
<td>Deployment Prerequisites</td>
<td>50</td>
</tr>
<tr>
<td>Installing and Configuring Foundation Services</td>
<td>50</td>
</tr>
<tr>
<td>Installing Metadata Services Schema for Oracle Web Services Manager</td>
<td>50</td>
</tr>
<tr>
<td>Configuring Oracle Web Services Manager</td>
<td>50</td>
</tr>
<tr>
<td>Configuring WebLogic with an External Provider</td>
<td>51</td>
</tr>
<tr>
<td>Configuring the API Adapter</td>
<td>51</td>
</tr>
<tr>
<td>Deploying the Web Service Application</td>
<td>51</td>
</tr>
<tr>
<td>Securing the Data Relationship Management Web Service</td>
<td>51</td>
</tr>
<tr>
<td>Configuring Policies in Oracle Web Services Manager</td>
<td>52</td>
</tr>
<tr>
<td>Configuring Data Relationship Management API Adapter for SSL (Optional)</td>
<td>52</td>
</tr>
<tr>
<td>Testing the Data Relationship Management Web Service Using Oracle Enterprise Manager</td>
<td>53</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>55</td>
</tr>
</tbody>
</table>
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 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

Send feedback on this documentation to: epmdoc_ww@oracle.com

Follow EPM Information Development on these social media sites:
LinkedIn - http://www.linkedin.com/groups?gid=3127051&goback=.gmp_3127051
Twitter - http://twitter.com/hyperionepminfo
Facebook - http://www.facebook.com/pages/Hyperion-EPM-Info/102682103112642
Google+ - https://plus.google.com/106915048672979407731/#106915048672979407731/posts
YouTube - http://www.youtube.com/user/OracleEPMWebcasts
Installation Prerequisites

Items to check:

- Oracle Data Relationship Management must be installed by a user who is logged in as an administrator.
- Intended host computers meet or exceed the minimum system requirements.

**Note:** For information on certified versions of platform components, refer to the Oracle Hyperion Enterprise Performance Management System Certification Matrix at http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html.

- Database server is installed and running on the database computer.
- Internet Information Services (IIS) is installed and operational on the Web server.
- 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

For more information, see:

- Architecture Options
- 64-bit Operating System
Architecture Options

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

Figure 1  Data Relationship Management Architecture
Figure 2  Data Relationship Management with Multiple Applications

Figure 3  Data Relationship Management with Multiple Application Servers

Installation Prerequisites 13
Figure 4  Data Relationship Management with External Authentication
Figure 5  Data Relationship Management with EPM Foundation
Figure 6  Data Relationship Management with Web Service Integrations

Installing Data Relationship Management

- DRM Console
- DRM Service
- Batch Client

- Engine
- Event Mgr

- Engine
- Event Mgr

- EPM Foundation

A: TCP/IP  B: Net.Ipc  C: Http/s

EPM Foundation does not need to be in a running state.
64-bit Operating System

When using a 64-bit operating system, such as Windows Server 2003 Enterprise x64 Edition, it is necessary to first install the 64-bit version of .NET Framework 4.0 before installing Data Relationship Management.

Windows Server 2008 Prerequisites

.NET Framework

When installing on Microsoft Windows Server 2008, you must install .NET Framework 4.0 from the management console.

To install .NET Framework 4.0:

1. From the Start Menu, select All Programs, Administrative Tools, and then Server Manager.
2. In the tree on the left, click Features.
3. Click the Add Features link on the right.
4 Select the .NET Framework 4.0 Features option.
5 Click Next.
6 Click Install.
7 Click Close after the installation completes.

IIS 6 Metabase Compatibility

To install IIS6 Metabase Compatibility on Windows Server 2008 SP2:
1 Open Administrative Tools, and then open Server Manager.
2 Select role: Web Server (IIS).
3 Click Add Role Service.
4 Select IIS 6 Metabase Compatibility.
5 Click Next.
6 Click Install.

Oracle Database Prerequisites

- If you are using an Oracle RAC database system, you must create the tablespaces with the appropriate RDBMS software prior to installation.
- Whether the scripts are run automatically or manually, the user must be logged in as SYSTEM. When you manually execute the database scripts, the User ID that was designated for Data Relationship Management database connectivity in the Repository Wizard is created in the RDBMS (if it does not already exist). The user is assigned a default tablespace of DRM_DATA and must have access rights to the following items:
  - Default tablespace (usually DRM_DATA)
  - UNLIMITED TABLESPACE
  - CONNECT
  - CREATE ANY SEQUENCE
  - CREATE USER
  - ALTER USER
- When you manually execute the database scripts, the user is logged in as the schema owner which, has a default tablespace of DRM_DATA. This user must have access rights to the following items:
  - Default tablespace (usually DRM_DATA) — this can be done after the install if the tablespaces were not created.
  - UNLIMITED TABLESPACE
  - DBA
  - CONNECT
CREATE ANY SEQUENCE
CREATE USER
ALTER USER

Note: You can change the schema owner name during the installation process.

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 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.

PDF Font Requirement for Asian Glyphs
To be able to see Asian glyphs in downloaded PDF files, the "Arial Unicode MS" font must be installed on the Web server.

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.

Additional Documentation
You can find Oracle Hyperion 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 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

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
- Integration with Oracle Hyperion EPM Architect
- API programs and SOA-based processes using the Data Relationship Management web service

The Foundation Services installation includes the following components that must be configured to enable these components for Data Relationship Management:

- Oracle WebLogic Server
- Oracle HTTP Server
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*.

For more information, see:

- Data Relationship Management CSS Bridge
- Deployment Scenarios For Data Relationship Management and Foundation Services

**Data Relationship Management CSS Bridge**

The Data Relationship Management CSS Bridge is used to communicate with Shared Services and must be installed when Foundation Services is used with Data Relationship Management. The following information and requirements are important for understanding the Data Relationship Management CSS Bridge. Also review Figure 4 on page 14.

- The CSS Bridge component is included with the Data Relationship Management Application Server installation component.
- The CSS Bridge must be run on a supported Microsoft Windows computer.
- If the designated CSS Bridge Host computer is not the Data Relationship Management application controller, then:
  - You must install the Data Relationship Management Application Server component on the CSS Bridge Host computer.
- A Foundation Services installation and deployment is required on the computer on which the CSS Bridge will be running.

**Deployment Scenarios for Data Relationship Management and Foundation Services**

Review Figure 5 on page 15 for more information on Data Relationship Management with Foundation Services.

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

**Scenario 1**

Computer 1: Data Relationship Management application controller, primary Foundation Services instance, and Data Relationship Management CSS Bridge

**Scenario 2**

- Computer 1: Data Relationship Management application controller
Installing Data Relationship Management

Before installing Data Relationship Management, review Figure 1 on page 12.

To install Data Relationship Management:

1. Navigate to the directory where you downloaded the installation program and double-click setup.exe.
2. Select the language for the installation and click OK.
3. If you do not already have Microsoft .NET Framework 4.0 installed, click Install to install it.
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, Web Server, Migration Utility, Batch Client, and the documentation.
   - Custom — Allows you to select the components to install. You can select from the following components:
     - DRM Application Server
     - DRM Web Server
     - DRM Migration Utility
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**.

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

See the following sections:

- Installing Secondary Engine Hosts
- Installing Secondary Data Relationship Management Web Server Hosts
- Installing Secondary API Adapter Hosts
- Installing Secondary Foundation Services Hosts

### Installing Secondary Engine Hosts

Before installing multiple application servers, review *Figure 3 on page 13*.

To install an optional secondary Data Relationship Management Engine Host computer, install the Data Relationship Management Application Server component on the secondary computer.

**Note:** The Data Relationship Management Web Server component is not required for an Engine Host.

**Note:** Do not launch the Data Relationship Management Configuration Console for configuration on the secondary server.
Installing Secondary Data Relationship Management Web Server Hosts

To install a secondary Data Relationship Management Web Server computer, install the Data Relationship Management Application Server and Web Server components on the secondary computer.

**Note:** The Data Relationship Management Web Server component is dependent on the Data Relationship Management Application Server component.

**Note:** Do not launch the Data Relationship Management Configuration Console for configuration on the secondary server.

Installing Secondary API Adapter Hosts

To install the API Adapter Host on a secondary computer, install the Data Relationship Management Application Server component on the secondary computer.

**Note:** The Data Relationship Management Web Server component is not required for an API Adapter Host.

**Note:** Do not launch the Data Relationship Management Configuration Console for configuration on the secondary server.

Installing Secondary Foundation Services Hosts

The following 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*. 
The Data Relationship Management Configuration Console is an application server configuration utility.

When you install Data Relationship Management, the Data Relationship Management Configuration Console is automatically installed. 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.

Configuring Foundation Services for Data Relationship Management

The Foundation Services installation includes several components which must be deployed and configured using the EPM Configurator tool before 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.

For more information, see:

- Configuring Secondary Foundation Services Hosts
- Configuring Shared Services with an External Provider
- Configuring Shared Services for Single Sign On
- Configuring CSS Mode for Data Relationship Management

**Configuring Secondary Foundation Services Hosts**

- The CSS Bridge component is included with the Data Relationship Management Application Server installation component.
- The CSS Bridge must be run on a supported Microsoft Windows computer.
- If the designated CSS Bridge Host computer is not the Data Relationship Management application controller, then:
  - You must install the Data Relationship Management Application Server component on the CSS Bridge Host computer.
  - The Windows 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 controller.
- A Foundation Services installation and deployment is required on the computer on which the CSS Bridge will be running.
- If a secondary 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.

Configuring Shared Services with an External Provider

To configure 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/olap-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 for Single Sign On


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 Shared Services. See “CSS” on page 37 and “Configuring Authentication Settings” on page 38.

Starting the Data Relationship Management Configuration Console

To open the 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

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. Applications can also run on multiple machines to distribute the processing of concurrent, long running operations. Each application has a controller, a set of engines, and a repository connection.
Before configuring multiple Data Relationship Management applications, review Figure 2 on page 13.

See the following sections:

- Creating an Application
- Application Controller
- Setting the Application Default Culture
- Date, Time, and Number Formatting
- Creating a Repository
- Copying a Repository
- Configuring Host Computers
- Configuring Authentication Settings
- Configuring EPM Registry Settings
- Configuring Scheduled Tasks
- Removing an Application

**Creating an Application**

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

1. 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.
   
      **Note:** If you have not created a repository, or need to upgrade the repository, you need to use the Repository Wizard. See “Creating a Repository” on page 30.

2. Click **Save Configuration**.
3. 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.

**Application Controller**

You must configure a computer to be the application controller for an application. Only one computer can be configured as the controller for an application. The computer that is the application controller runs the Data Relationship Management Process Manager program, which controls all Data Relationship Management processes on all computers configured in the Data Relationship Management application.
The application controller computer also has the Data Relationship Management configuration file (`drm-config.xml`). No matter how many computers are configured for a Data Relationship Management application, only one configuration file will exist. All configuration for an application must be done on the application controller computer.

**Server Port Number**

To communicate successfully, the Data Relationship Management Windows Service on the primary and all secondary servers must use the same port number for the minimum port range (5200 by default). The Data Relationship Management primary server dynamically allocates other required ports within the range as needed.

**Setting the Application Default Culture**

You can set the default culture used for each Data Relationship Management application.

- 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
     - ko-KR – Korean
     - zh-CHS – Simplified Chinese

**Date, Time, and Number Formatting**

Formatting of date, time, and number property data values in the 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 server computer (on the Data Relationship Management Application Controller server).

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.

**For Example** – A Data Relationship Management Web Client browser language is set to "en-US". You are logged into the Data Relationship Management server as the Data Relationship Management service logon account and the corresponding Regional Options culture "English (United States)" has the short date format "MM/dd/yyyy". Dates in the Data Relationship Management client user interface are displayed in the format "MM/dd/yyyy".

**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. For information on upgrading, see “Upgrading an Existing Data Relationship Management Application” on page 60.

➢ 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” on page 33.
   - 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.
- **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**.

<table>
<thead>
<tr>
<th>Database Provider</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Connection</td>
<td><img src="//localhost:1521/orcl" alt="Connection Format" /></td>
</tr>
<tr>
<td>User ID</td>
<td>sa</td>
</tr>
<tr>
<td>Password</td>
<td>**********</td>
</tr>
</tbody>
</table>

| Connection Timeout (Seconds) | 60 | Command Timeout (Seconds) | 900 |

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” on page 32.

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.

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 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 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**

The Repository Wizard in the Configuration Console provides the ability to copy a repository from a current release to a different repository running on the same or a different database provider.

- **Copy path option 1:**
  - Run the Create a New Repository and Copy or Upgrade an Existing Repository options simultaneously.

    **Note:** Refer to the description on the Repository Wizard Source Connection page for important information on the different copy methods for a current release repository.

- **Copy path options 2:**
  1. Run the Create a New Repository option or manually run the create repository SQL scripts.
  2. Run the Copy or Upgrade an Existing Repository option using the new repository created in step 1 as the target connection.

**Configuring Host Computers**

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 scalability, you can optionally distribute Data Relationship Management Engine Hosts, API Adapter Hosts, Web Servers, and the CSS Bridge Host across multiple computers. For configuration details, refer to the applicable host computer section:

- Process Manager
- Event Manager
- Engine Hosts
- API Adapter Hosts
- Web Servers
- CSS
- SMTP Server

**Process Manager**

➤ To configure a Process Manager computer:

1. Enter the computer name and port number.

   **Note:** The Process Manager host must be on the Data Relationship Management application controller computer. The port number can be changed.

2. For **Engine Startup Timeout**, enter the number of seconds for the Process Manager to wait when starting a 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.

3. For **Total SRO Engines**, enter the total number of Short read-only engines.

   **Note:** The default value for the short read-only engines is 1 and should not be changed unless otherwise directed by Oracle Support.

**Event Manager**

➤ To configure the Event Manager computer, enter the computer name.

**Note:** Oracle recommends running the Event Manager on the application controller.
Engine Hosts

To configure an Engine Host computer, enter the computer name and maximum number of Data Relationship Management engines to be started on the host.

API Adapter Hosts

API Adapter components are included with the Data Relationship Management Application Server installation component. An API Adapter Host can be the Data Relationship Management application controller or a secondary Data Relationship Management computer.

Note: An API Adapter host is only required if you are going to access Data Relationship Management using the Web Services API.

To configure the Data Relationship Management application controller as the API Adapter Host, enter the application controller computer name, port number, and a certification number to enable SSL. Click the plus sign to add a host computer.

Web Servers

On the UI Web Servers tab, you list the servers that are configured to run the 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. 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.

2. 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.

3 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

**CSS**

➢ To configure CSS:

1 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” on page 44. For information on setting authentication settings, see “Configuring Authentication Settings” on page 38.

   - **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.

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

   - **JVM Path** – The path to the java virtual machine (jvm.dll). Default location is C:\Oracle\Middleware\EPMSystem11R1\common\JRE\Sun\1.6.0\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 server or the application controller.

2 **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\awbutil.jar
- 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\wlserver_10.3\server\lib\wlsqllserver.jar
- C:\Oracle\Middleware\modules\javax.servlet_1.0.0.0_2-5.jar

**SMTP Server**

The Data 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 Governance notifications to work.

➢ **To configure an SMTP server:**

1 Select **Enable SMTP**.

2 Specify the host name of the SMTP server.

3 Specify the SMTP port number.

4 Select **Requires SMTP Authentication** and enter the user name and password for the SMTP server.

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

6 Enter the sender email address.

**Configuring Authentication Settings**

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

➢ **To configure authentication settings:**

1 Click **Load Settings** to populate the current settings as saved in the Data Relationship Management system preferences.
Select the method for authentication:

- **Internal** – Managed fully by Data Relationship Management.
- **CSS** (Common Security Services) – Centralized support for external user directories using Shared Services.
- **Mixed** – Allows authentication option (Internal or CSS) to be specified by the user.

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.

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.

Click **Save Settings**.

**Configuring EPM Registry Settings**

If you are using Performance Management Architect to import hierarchies, nodes, and properties from Data Relationship Management, you must register the Data Relationship Management application instance in the Oracle Hyperion Shared Services Registry. The Data Relationship Management application and Oracle Hyperion EPM Architect must be registered to the same Shared Services instance.

**Note:** The CSS Bridge component must be enabled and the application that you are registering or unregistering must be running.

To register a Data Relationship Management application:

1. **On the EPM Registry tab, specify the Data Relationship Management Web service by entering 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

   This information is combined into a URL; for example, http://servername:9000/oracle-epm-drm-webservices
where http is the protocol, servername is the host computer name of the Web service, 9000 is the port number, and oracle-epm-drm-webservices is the name of the WebLogic application for the Web service.

2 Select the Data Relationship Management API adapter URL.

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

4 Click Register.

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.

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

2 Select the application and then click Scheduled Tasks.

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

4 Click Load Settings.

Setting a Blackout Window

You can set a blackout window for times when you do not want scheduled purges to run.

To select a blackout window when scheduled purges should not run:

1 On the Schedule Tasks tab, enter the start time for the blackout and then select how long (in hours) the blackout should last.

2 Click Load 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

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

- To save settings and start the Data Relationship Management service:
  1. On 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 controller server.

Launching Data Relationship Management in a Web Browser

- To launch 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
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 1  Configuration Settings

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuredServers</td>
<td>Specifies the admin-configured connections.</td>
</tr>
<tr>
<td></td>
<td>Default value is net.tcp://localhost:5210/Oracle/Drm/ProcessManager where localhost is the computer and 5210 is the configured process manager port.</td>
</tr>
<tr>
<td>maximumExceptionsOnImport</td>
<td>If the Continue After Error option is selected, specifies the maximum number of exceptions that can be generated during a load. Specify an integer greater than 0. The default value is 1000.</td>
</tr>
<tr>
<td>showExceptionDetail</td>
<td>Specifies whether detailed exception information is displayed on the error page.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>enableAboutPage</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

For more information, see Increasing Upload File Size.

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:

```xml
<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 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.
2. Configure Data Relationship Management applications and host computers using the procedure described in “Configuring Data Relationship Management Applications” on page 27.
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
Add the following Forward and Reverse Proxy directives.

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

# Do not forget ProxyPassReverse for redirects
```

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 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 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 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).

Use the following steps to install and configure SSO:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Install Data Relationship Management.</td>
<td>See “Installing Data Relationship Management” on page 22.</td>
</tr>
</tbody>
</table>
4. In the Data Relationship Management Configuration Console, configure Data Relationship Management for CSS authentication mode and enable SSO.

   See “Configuring Host Computers” on page 34.

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” on page 45.

For more information, see Web Access Management.

**Web Access Management**

The 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 Data Relationship Management Web application. 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 “Configuring the Access System and Protecting Resources” in the OAM Access Administration Guide.

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

- Install and configure Oracle Access Manager 10g Webgate for IIS on the Data Relationship Management Web server
- Set up Oracle HTTP Server for load balancing the Data Relationship Management Web server and install Oracle Access Manager 11g Webgate for OHS

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

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” at http://www.oracle.com/technetwork/middleware/ias/downloads/101401-099957.html.

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

Online Help content for Data Relationship Management is served from a central Oracle download location, which reduces the download and installation time for Data Relationship Management.

You can choose to install and configure the Help feature in your own environment if all users will not have internet access to Online Help. During the installation process, select the "DRM Documentation" component to install the Help feature on the Data Relationship Management Web server.

**Note:** If you require accessible Help that is Section 508 compliant, you must install and configure Help to run locally.

To configure the Help feature to run on the Data Relationship Management Web server:

1. Open the Data Relationship Management Configuration Console.
2. Select the Host Machines tab and then select the UI Web Servers tab.
4. In Help Base URL, enter the URL as `http://Web_Server_Name/drm-web-client/documentation` where **Web_Server_Name** is the name of the host machine.

**Note:** The Help Base URL points to the root of the virtual folder on a Web server where the help can be accessed internally. The documentation folder can be transferred manually to another Web server, and the Help Base URL would need to be updated to point to the correct root URL.

5. Click the test URL to verify the link.
6  Save the changes to the console.
Deploying and Configuring the Data Relationship Management Web Service API

In This Chapter

System Requirements ................................................................. 49
Deployment Prerequisites .......................................................... 50
Deploying the Web Service Application ....................................... 51
Securing the Data Relationship Management Web Service ................. 51
Testing the Data Relationship Management Web Service Using Oracle Enterprise Manager .... 53
Troubleshooting .................................................................... 55

The 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 Shared Services.

Before deploying the Data Relationship Management Web Service API, review Figure 6 on page 16 and Figure 7 on page 17.

System Requirements

- Oracle WebLogic Server 11g
- Data Relationship Management API Adapter
- Oracle Web Services Manager (OWSM)
- Shared Services
- An external user directory such as Oracle Internet Directory or Microsoft Active Directory

Note: See the Oracle Enterprise Performance Management System Certification Matrix for the latest system requirements.
Deployment Prerequisites

The following sections include prerequisites for deploying the Data Relationship Management Web Service API:

- Installing and Configuring Foundation Services
- Installing Metadata Services Schema for Oracle Web Services Manager
- Configuring Oracle Web Services Manager
- Configuring WebLogic with an External Provider
- Configuring the API Adapter

Installing and Configuring Foundation Services

To support Web Services (WS) Security, Foundation Services must be installed and Data Relationship Management must be configured to use Shared Services for authentication. WebLogic and the Oracle Web Services Manager components are installed when you install Foundation Services. For information on installing Oracle Hyperion Foundation Services, see “Foundation Services” on page 20.

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

You configure Oracle Web Services Manager by running the Oracle Fusion Middleware Configuration Wizard and configuring a WebLogic domain. You then select the products that you want to configure in that domain.

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 Data Relationship Management Web Service application deployed on Weblogic must be configured to access the same user directory that is configured with Shared Services for externally authenticating users. This configuration is required to support WS-Security policies available in Oracle Web Services Manager.

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 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” on page 34.

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 Service Application

The oracle-epm-drm-webservices.ear file should be deployed to an existing WebLogic domain. The oracle-epm-drm-webservices.ear file is located in the %EPM_ORACLE_HOME%\products\DataRelationshipManagement\api directory of the application controller machine.

Deploy oracle-epm-drm-webservices.ear to WebLogic. 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/technetworkindexes/documentation/index.html#middleware.

Securing the Data Relationship Management Web Service

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 Data Relationship Management Web services:
### Purpose

| Integration with Oracle Hyperion EPM Architect | oracle/wss11_saml_or_username_token_with_message_protection |
| Integration with E-Business Suite General Ledger | oracle/wss_username_token_service_policy |
| Integration with Oracle Fusion Accounting Hub | oracle/wss_saml_or_username_token_service_policy |
| Workflow Development Kit | oracle/wss11_saml_or_username_token_with_message_protection |
| Custom API Programs or Integrations | One of the following:  
  - 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 |

For more information, see:

- Configuring Policies in Oracle Web Services Manager
- Configuring Data Relationship Management API Adapter for SSL


### 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.

### Configuring Data Relationship Management API Adapter for SSL (Optional)

The Data Relationship Management Web Service uses the API Adapter to communicate with the Data Relationship Management server.

1. To configure the Data Relationship Management API Adapter for SSL:

   - Install an SSL Certificate and map the API Adapter port to this certificate.
Note: The Data Relationship Management API Adapter uses the Windows Communication Foundation (WCF). For more information regarding WCF and working with certificates, see http://msdn.microsoft.com/en-us/library/ms731899%28v=VS.90%29.aspx.

a. Obtain an SSL certificate. For a production environment, a certificate should be obtained from a reputable Certificate Authority vendor. For a test environment, self-signed certificates can be generated using the Windows MakeCert utility.
b. Import the certificate into the Trusted Root Certification Authorities store using the MMC Snap-in.
c. Obtain a thumbprint value from the certificate.
d. Configure the API Adapter (WCF) port with an SSL Certificate. For instructions, see http://msdn.microsoft.com/en-us/library/ms733791%28v=VS.90%29.aspx.

Note: The default port for the API Adapter is 5240.

2 Configure API Adapter for HTTPS / SSL. To enable SSL, on the API Adapter Hosts tab of the Data Relationship Management Configuration Console, enter the Certificate Name.

3 Test to make sure HTTPS/SSL is working.
   a. After the changes described above have been completed, restart the Data Relationship Management Service. This can be done from the Data Relationship Management Configuration Console.
   b. From a Web browser, access the Data Relationship Management API Adapter WSDL using the following URL: https://drm host name:5240/Oracle/Drm/APIAdapter?wsdl where drm host name is the name of the computer where the Data Relationship Management Server is running.

Note: The protocol is https instead of http. The http protocol can be used to access the wsdl when HTTPS/SSL is not enabled.

Testing the Data Relationship Management Web Service Using Oracle Enterprise Manager

To test the Web Service using Oracle Enterprise Manager:

1 Ensure that the 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.

1. 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.

2. 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

3. From Operation, select an operation; for example getSysPrefs.

4. 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 Shared Services.

5. 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:

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

6. 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.

7. Click Test Web Service.

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

8. After testing is complete, re-attach the required production policy.
### Troubleshooting

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle EPM Foundation Agent Error in request: begin session</td>
<td>Shared Services doesn't contain the user identity.</td>
<td>Ensure Data Relationship Management is configured with the same User directory as used by the WebLogic realm.</td>
</tr>
<tr>
<td>(message: Cannot begin session. EPMCSS-00301: Failed to authenticate user. Invalid credentials. Enter valid credentials.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>javax.xml.ws.soap.SOAPFaultException: FailedAuthentication:</td>
<td>User identity is not present in WebLogic security realm.</td>
<td>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.</td>
</tr>
<tr>
<td>The security token cannot be authenticated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>javax.xml.ws.WebServiceException: Failed to access the WSDL at:</td>
<td>Host or port is incorrect. The Web service is not running on the WebLogic domain.</td>
<td>Verify the Data Relationship Management Web service is deployed and running on the WebLogic domain. Modify the host/port reference in the WSDL URL.</td>
</tr>
<tr>
<td>Error while trying to communicate with DRM API Adapter at:</td>
<td>Host or port is incorrect. The API adapter is not running or configured correctly.</td>
<td>Verify the API adapter is configured and running. Change the API adapter URL in the client program/application to the correct value.</td>
</tr>
<tr>
<td><a href="http://localhost:5240/oracle/Drm/APIAdapter/">http://localhost:5240/oracle/Drm/APIAdapter/</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>javax.xml.ws.soap.SOAPFaultException: SOAP must understand error:</td>
<td>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”</td>
<td>Attach either a global or local policy to the Data Relationship Management Web service. Follow the steps in the OWSM troubleshooting section: <a href="http://download.oracle.com/docs/cd/E12839_01/web.1111/b32511/diagnosing.htm#CHIDIDCHA">http://download.oracle.com/docs/cd/E12839_01/web.1111/b32511/diagnosing.htm#CHIDIDCHA</a></td>
</tr>
</tbody>
</table>
Upgrading is the process of deploying a new software release and moving applications and data from the earlier deployment to the new deployment.

It is important that you review the Data Analysis and Data Conversion sections to have a complete understanding of how data is affected during an upgrade from a Data Relationship Management release prior to 11.1.2.

**Supported Upgrade Paths**

You can upgrade to this release of Data Relationship Management from the following releases:

- 9.2.x
- 9.3.x
- 11.1.x

**Note:** If you are upgrading from release 11.1.2, install this release over the earlier release. If you are upgrading from a release before 11.1.2, you must first manually uninstall the old release and then install the new release.

The Repository Wizard in the Data Relationship Management Configuration Console provides various options for upgrading a Data Relationship Management repository from an earlier release.

The following sections describe the high-level options for upgrading or copying a repository:

- Repository Upgrade Paths for 9.2.x, 9.3.x, and 11.1.1.x
- Repository Upgrade Paths for 11.1.2.0.x, 11.1.2.1.x, and 11.1.2.2.x
- Repository Upgrade Path for 11.1.2.3
For detailed instructions, see “Upgrading an Existing Data Relationship Management Application” on page 60.

Repository Upgrade Paths for 9.2.x, 9.3.x, and 11.1.1.x

- Upgrade path option 1:
  - Run the Create a New Repository and Copy or Upgrade an Existing Repository options simultaneously.
- Upgrade path option 2:
  1. Run the Create a New Repository option or manually run the create repository SQL scripts.
  2. Run the Copy or Upgrade an Existing Repository option using the new repository created in step 1 as the target connection.

Repository Upgrade Paths for 11.1.2.0.x, 11.1.2.1.x, and 11.1.2.2.x

- Upgrade path option 1:
  1. Add a new application and specify the repository connection information for an existing 11.1.2.0.x, 11.1.2.1.x, or 11.1.2.2.x repository.
  2. Run Apply Updates on the application.
- Upgrade path option 2:
  - Run the Create a New Repository and Copy or Upgrade an Existing Repository options simultaneously.
- Upgrade path option 3:
  1. Run the Create a New Repository option or manually run the repository creation SQL scripts.
  2. Run the Copy or Upgrade an Existing Repository option using the new repository created in step 1 as the target connection.

Repository Upgrade Path for 11.1.2.3

1. Add a new application and specify the repository connection information for an existing 11.1.2.3 repository.
2. Run Apply Updates on the application.
# Upgrading Checklist

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

## Table 2  Upgrading Checklist

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference</th>
</tr>
</thead>
</table>
| 1. Review release compatibility, system requirements, and other prerequisites for this release. | - "Installation Prerequisites" on page 11  
- Oracle Hyperion Enterprise Performance Management System Installation Start Here |
| 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 Shared Services, you must upgrade the Oracle Hyperion Shared Services installation before upgrading the Data Relationship Management. For more information, see the 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 from release 11.1.2, you do not need to uninstall the earlier release. Install this release over the earlier release. If you are upgrading from a release before 11.1.2, 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" on page 22.                                                                                   |
| 7. Configure Data Relationship Management.                           | Use the Data Relationship Management Configuration Console to configure the new installation. See "Upgrading an Existing Data Relationship Management Application" on page 60. |
| 8. Redeploy the Web Service for this Data Relationship Management release. | The name of the Web service application in WebLogic is "oracle-epm-drm-webservices" by default.                                |
| **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 |
| 9. Optional: Deploy and configure the Web Service.                    | Deploying and Configuring the Data Relationship Management Web Service API                                                             |
| 10. Start Data Relationship Management services.                     |                                                                                                                                          |
Upgrading an Existing Data Relationship Management Application

You must update the repository information for all existing applications. You can upgrade applications from prior Data Relationship Management releases and copy applications from the current release.

Note: The following procedure documents a common upgrade path. Because there are several paths for upgrade, not all of the steps below are applicable to some of the upgrade paths.

For release-specific upgrading information, see “Repository Upgrade Paths for 9.2.x, 9.3.x, and 11.1.1.x” on page 58, “Repository Upgrade Paths for 11.1.2.0.x, 11.1.2.1.x, and 11.1.2.2.x” on page 58, and “Repository Upgrade Path for 11.1.2.3” on page 58.

For more information, see:
- Data Analysis
- Working with External Connections
- Data Conversion

To upgrade an existing Data Relationship Management application:

1. Select Start, then Programs, then Oracle EPM System, then Data Relationship Management, and then Configuration Console.
2. Select an application to upgrade or add a new application to upgrade.

Note: You must update repository information for all existing applications before starting the Data Relationship Management service.

4. Select these options and click Next:
   - Create a New Repository
   - Copy or Upgrade an Existing Repository
5. On the Source Connection page, do the following:
   a. Select a database provider: Oracle or SQL Server.
   b. Enter the connection to the source repository. This is the database from which data is copied. Nothing is changed in this database.
   c. Enter a user ID and password for a user who can read from this database.
   d. 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.
Caution! To ensure that a timeout does not occur, set the Command Timeout to zero.

e. Click **Test Connection**.

6 Click **Next**.

7 **On the Target Connection page**, do the following:
   - Select the database provider: Oracle or SQL Server.
   - Enter the connection to the target database where the upgraded repository will reside.
   - Enter the user ID and password for an administrator who has rights to create a database schema and data files.
   
   **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.

Caution! To ensure that a timeout does not occur, set the Command Timeout to zero.

- Click **Test Connection**.

8 Click **Next**.

9 **On the Repository Analysis screen**, review and make changes to:
   - **Versions** — Select the versions to upgrade; de-select versions that should not be included in the upgrade.
   - **Exports** — Set up file connections, database connections, and include connections for the exports to be upgraded. You can make changes at the top of the screen for all exports or make changes to individual exports.
   - **Books** — Set up pre file connections, post file connections, and combined file connections for the books to be upgraded. You can make changes at the top of the screen for all books or make changes to individual books.
   - **Imports** — Set up import file connections for the import to be upgraded. You can make changes at the top of the screen for all imports or make change to individual imports.
   - **Invalid Property References** — These property references are invalid and may result in unexpected behavior after upgrade.

**Note:** For additional information on these objects and how data conversion works during upgrade, see “Data Analysis” on page 63 and “Data Conversion” on page 66.

10 Click **Next**.

11 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” on page 32.

12 On the Repository User and Data File Settings page, enter the user id and password which will be created as the schema owner for the Data Relationship Management repository.

13 Accept the default tablespace settings or make changes and click Next. For information on default sizing of the repository, see “Data Analysis” on page 63.

   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.

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

   Note: The default Administrator user is ADMIN but you can change the default Admin user.

   Caution! If you are upgrading 11.1.2.x applications, the password for an existing ADMIN user is not overwritten with the password entered here.

15 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.

16 Click Next.

17 On the Copy Repository Confirmation page, review the settings and click Next to start the copy process.

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

18 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.

19 On the Repository Operation Complete screen, click Finish.

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

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

For additional application configuration tasks, see:

   - Configuring Host Computers
   - Configuring Authentication Settings
   - Saving Configuration Settings and Starting the Service
Data Analysis

The Repository Analysis page provides information about the source repository so that decisions can be made that affect size and objects in the new repository. The Analysis Summary section provides an overview of the analysis. The space requirements are broken down into different segments and are given as a whole so that the user can better understand the space requirements for the new repository. Sizing found here is automatically applied to the Repository User and Data File settings page when the calculated space requirements are greater than 200 MB for each default tablespace in an Oracle repository, or greater than 5 MB for the data and log files in a SQL Server repository. The Object Analysis section displays outstanding issues that need to be addressed prior to moving on with the upgrade.

- **Versions** — Displays the versions and provides the opportunity to deselect versions that should not be included in the upgrade. Deselecting a version affects the space and count values in the Summary section.

- **Exports** — Displays any exports that need special attention. Exports that require an External Connection for results or other external files are included here. Exports that are no longer supported, such as custom exports, are included here as well. If no External Connection is provided, the export is configured as a client file export. For more information on External Connection, see “Working with External Connections” on page 64.

- **Books** — Displays books that require an External Connection for combined files, Pre files, and or Post files. If no External Connection is provided, the export is configured without utilizing a combined file. For more information on External Connections, see “Working with External Connections” on page 64.

- **Imports** — Displays imports that require an External Connection for its input file. If no External Connection is specified, the import is configured as using a client input file. For more information on External Connections, see “Working with External Connections” on page 64.

- **Invalid Property References** — Displays property references that may cause unexpected behavior in the Data Relationship Management system. These invalid references are generally only caused by updating the Data Relationship Management database directly. The following scenarios are included here.

  For the following two scenarios, during repository analysis, the property definition is flagged and its data values that can no longer be referenced are considered abandoned. When upgrading an 11.1.1.x source, the abandoned records are not copied to the new repository. When upgrading an 11.1.2.x source, the abandoned records are copied to the new repository but are not displayed in the Web Client UI and a warning is displayed in the Windows Event Viewer Application log on the application controller when the Data Relationship Management service is started.

  - A global property that has been referenced as a local property in the Property_Local or RM_Node_Prop_Local tables.
  - A local property that has been referenced as a global property in the Property_Global or RM_Node_Prop_Global tables.
For example, records in the 11.1.1.x Property_Local table will not be copied for property definitions that are now set as global. Likewise, records in the 11.1.1.x Property_Global table will not be copied for property definitions that are now set as local.

For the following scenarios, during repository analysis, the property definition is flagged to alert the user only. The property definition is copied to the upgraded database as it exists in the source database but should be reviewed for validity.

- A derived global property that contains a deriver parameter that references a local property
- A global formula property that contains a formula that references a local property in one of the following formula methods:
  - IsRangeListSubset
  - NodePropValue
  - OrigPropValue
  - ParentPropValue
  - PropControllingHier
  - PropMaxValue
  - PropMinValue
  - PropValue
  - RangeListContains
  - ReplacePropValue
  - Stuff
- A global lookup property that points to a local property as the lookup property

---

**Working with External Connections**

External Connections are used to access server file locations, FTP locations, and database tables. You can create and apply default connections and you can apply connections individually. After you create a file connection, it can be referenced by any object that requires a file connection. For example, if you create a connection for an export, that connection is also available in the imports section. You can multi-select and apply or you can select all and apply.

For more information, see:
- Creating External Connections
- Applying External Connections

---

**Creating External Connections**

You can create external connections on a specific row in the analysis or at the top of the analysis screen in the File Connections field. In both places, you click **“** to open the Create Connection
dialog box. When you create external connections at the row level, the connection is automatically applied to the row.

To create an external connection to a server file:

1. In the File Connections field, click "...".
2. Enter a name for the connection and, optionally, a description.
3. For Connection Type, select Server File.
4. Enter the UNC path to the server file. Click "..." to test the server connection.
5. Click OK.

To create an external connection to an FTP file:

1. In the File Connections field, click "...".
2. Enter a name for the connection and, optionally, a description.
3. For Connection Type, select FTP.
4. Enter the host server. Click "..." to select a test the server connection.
5. Enter a valid User ID and Password for the server.
6. Click OK.

To create an external connection to a database table:

1. In the File Connections field, click "...".
2. Enter a name for the connection and, optionally, a description.
3. Select the database provider: Oracle or SQL Server.
4. Enter the connection string to the database server.
5. Enter a User ID and Password for the server.

Note: You can click "..." to test the connection to the database.
6. Click "..." to load database tables.
7. Select database tables for the external connection.
8. Click OK.

Applying External Connections

Note: When you create external connections at the row level, the connection is automatically applied to the row. For information, see “Creating External Connections” on page 64.
To apply external connections to objects:

1. In the File Connections field, click and select an external connection to apply.
2. Select rows to which to apply the external connection.

*Note:* You can use **Shift + Click** and **Alt + Click** to select multiple rows. To apply the selected external connection to all rows, click **Select All**.

### Data Conversion

The following sections describe how data is converted during an upgrade:

- Users
- Transactions
- Exports
- Imports
- External Connections
- Properties

### Users

The role assigned to an ADMIN user is reset to all roles. Also, the password expiration date is reset to the current date plus the duration set in system preferences.

*Caution!* If you are upgrading 11.1.2.x applications, the password for an existing ADMIN user is not overwritten with the password entered here.

The Data Relationship Management upgrade process uses the following user type mappings:

<table>
<thead>
<tr>
<th>Old User Type</th>
<th>Assigned Functional Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Access Manager, Application Administrator, Data Manager, Workflow User</td>
</tr>
<tr>
<td>Functional</td>
<td>Data Manager, Workflow User</td>
</tr>
<tr>
<td>Security</td>
<td>Access Manager</td>
</tr>
<tr>
<td>User</td>
<td>Interactive User, Workflow User</td>
</tr>
</tbody>
</table>
Transactions

- The Data Relationship Management user interface displays date and time in local time and format according to the user’s session. When converting timestamp values from releases prior to 11.1.2, the following rules apply:
  - Timestamps are converted to UTC using the offset of the time zone in which the Data Relationship Management Configuration Console is running. If the console is running in a time zone that is different than the time zone in which the pre-11.1.2 release source data was written, then the converted dates could be earlier or later by one or more hours.
  - Releases prior to 11.1.2 did not consistently apply daylight savings time, therefore all transaction dates are converted using the appropriate offset dictated by the time zone in which the Data Relationship Management Configuration Console is running. If the date falls in a standard time period for the time zone of the console, then the standard UTC offset is applied. If the date falls in a daylight savings time period for the time zone of the console, then the daylight savings UTC offset is applied. For example, in the Eastern time zone, the standard UTC offset is -5 hours; during daylight savings time periods, the offset is -4 hours. For all new data added after the repository is upgraded, the stored dates also reflect the applicable standard and daylight savings UTC offsets.
  - Transaction records for deleted versions in the source repository are not copied to the target repository, thus the number of Transaction History records copied may not match the row count in the target RM_Transaction table.
  - If you deselect versions, transactions belonging to those versions are not copied.

The Export Run transaction type stores the export name in the Object Name field instead of the Property Abbrev field.

The Data Relationship Management upgrade process uses the following transaction name mappings:

<table>
<thead>
<tr>
<th>Old Transaction Name</th>
<th>New Transaction Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automator Run</td>
<td>Action Script Run</td>
</tr>
<tr>
<td>Migration Extract</td>
<td>Migration Export</td>
</tr>
<tr>
<td>Migration Load</td>
<td>Migration Import</td>
</tr>
<tr>
<td>Add System Category</td>
<td>Admin Add Hierarchy Group</td>
</tr>
<tr>
<td>Update System Category</td>
<td>Admin Update Hierarchy Group</td>
</tr>
<tr>
<td>Delete System Category</td>
<td>Admin Delete Hierarchy Group</td>
</tr>
</tbody>
</table>

Exports

The following sections explain how exports are upgraded:
Preview Exports
Exports that have the output mode of Preview are directly migrated to a Client File target device.

Database Exports
To use database exports, updated database connection information is required to create new External Connections. You can provide connection information for each database export, which facilitate the creation of new External Connections. If you choose to skip this step during the upgrade process, the database parameter information for the export is retained and migrated, but the output mode is set to Client File so that the export is in working order. After the system is up and running, new connections can be created and the exports can be configured to use them.

File Exports
File locations in systems prior to this release are configured in context of the client. Since the new system is a Web application, exports need to generate files based on the context of the server. For exports with the File output mode, the upgrade process allows you to provide file location information to facilitate new External Connections that map to a UNC path. If you choose to skip this step during the upgrade process, the filename is retained and migrated, but the output mode of the export is set to Client File. After the upgrade process, a proper External Connection can be created, and the export can be configured to use it.

Ancestor Exports
Ancestor exports are converted to Generation exports with appropriate settings to return the equivalent results as in the original Ancestor export.

Export Books
Export books containing file information are treated much like File Exports. During the upgrade process, you can create external connections to be used for the combined file, Pre file and Post file for the book. If you choose to skip this step during the upgrade process, the book is set to output to a client file.

Imports
Systems prior to this release allowed users to save import file locations and log file locations in context of the client application. In this release, file locations are now saved in context of the server using an External Connection, or an import can be saved to be able to choose a local file at runtime. During the upgrade process, you are given the opportunity to supply connection information that is used to create new External Connections. If you choose to skip this step during the upgrade process, the import requires that you choose a local import file at runtime. The log file is no longer saved to a file. The import results are rendered on the page, and if desired, you can download the results.
**External Connections**

External connections that were added on the Analysis page are inserted in to the new database and referenced by the metadata objects for which they were selected.

**Properties**

The Data Relationship Management 11.1.2.1 release introduced namespaces for property definitions. The upgrade process for a pre-11.1.2.1 application automatically converts derived property formulas with explicit property name references to use the appropriate namespace prefix (Custom for user-defined properties or Core for system-defined properties).

**Applying Updates to an Application**

1. 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**

**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 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 11.1.2.1 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 “Upgrading 11.1.2.1 API Programs” in the *Oracle Data Relationship Management API Guide* for a list of API changes between product releases and for instructions on regenerating Web service proxy classes.

API programs used with Data Relationship Management releases prior to 11.1.2 must be manually modified to use the Web service API offered in this release. Enhancements that have been made to the Web service API are covered in the *Oracle Data Relationship Management New Features*. For more information on using the Web service API, see the *Oracle Data Relationship Management API Guide*. See “Upgrading Pre-11.1.2 API Programs” in the *Oracle Data Relationship Management API Guide* for a mapping of pre-11.1.2 API operations to those available in the Web service API for this release.
Monitoring Data Relationship Management Applications

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

Application status information is located on the following tabs:

- **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.
- **Loaded Versions** – You can view the name of each version and the engines for each version.
- **Recent Events** – You can view recent application events, such as VersionLoaded, ImportFinished, and UpdateUserRole, and the time that each event took place.
- **Current Sessions** – You can view the user names logged into the application, including the time of login and the time of last activity.

Machine status information is located on the following tabs:

- **Machine Information** – You can view the machine name, operating system, version, time the machine started running, and the 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 application and machine monitoring 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. Do one of the following:
   - To view application monitoring information, select an application and then click the **Application Status** tab. Use the tabs noted above to view information for the application.
   - To view machine monitoring information, expand an application and select the computer name. Use the tabs noted above to view information for the application.