

Oracle® Hyperion Data Relationship Management, Fusion Edition

Oracle® Hyperion Data Relationship Steward

Oracle® Hyperion Data Relationship Management for Oracle Hyperion Enterprise Planning Suite

Oracle® Hyperion Data Relationship Management for Oracle Hyperion Financial Close Suite

Oracle® Hyperion Data Relationship Management for Customer Hub

Oracle® Hyperion Data Relationship Management Read Only Access

Installation Guide

RELEASE 11.1.2.1

Data Relationship Management Installation Guide, 11.1.2.1

Copyright © 1999, 2011, Oracle and/or its affiliates. All rights reserved.

Authors: EPM Information Development Team

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS:

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Documentation Accessibility	5
Chapter 1. Installing Data Relationship Management	7
Installation Prerequisites	7
64-bit Operating System	8
Windows Server 2008 Prerequisites	8
Oracle Database Prerequisites	8
SQL Server Database Prerequisites	9
Additional Documentation	9
About Middleware Home and EPM Oracle Home	9
Foundation Services	10
Installing Data Relationship Management	11
Troubleshooting	11
Chapter 2. Configuring Data Relationship Management	13
Configuring Foundation Services for Data Relationship Management	13
Configuring Shared Services with an External Provider	13
Configuring Shared Services for Single Sign On	14
Configuring CSS Mode for Data Relationship Management	14
Configuring Data Relationship Management Applications	14
Application Controller	14
Starting the Data Relationship Management Console	15
Simple Configuration Scenario	15
Creating a Repository	15
Configuring Host Computers	19
Configuring Authentication Settings	24
Saving Configuration Settings and Starting the Service	25
Launching Data Relationship Management in a Web Browser	25
Configuring the Migration Utility	25
Load Balancing Data Relationship Management Web Applications	26
Using Single Sign On with Data Relationship Management	27
Web Access Management	28

Terminating SSL at the Web Server	29
Chapter 3. Deploying and Configuring the Data Relationship Management Web Service API	31
System Requirements	31
Deployment Prerequisites	31
Installing and Configuring Foundation Services	31
Installing Metadata Services Schema for Oracle Web Services Manager	32
Configuring Oracle Web Services Manager	32
Configuring Weblogic with an External Provider	33
Configuring the API Adapter	33
Deploying the Web Service	33
Securing the Data Relationship Management Web Service	33
Configuring Policies in Oracle Web Services Manager	34
Configuring Data Relationship Management API Adapter for SSL (Optional)	34
Testing the Data Relationship Management Web Service Using Oracle Enterprise Manager	35
Troubleshooting	36
Chapter 4. Upgrading a Data Relationship Management Installation	39
Supported Upgrade Paths	39
Repository Upgrade Paths for 9.2.x, 9.3.x, and 11.1.1.x	40
Repository Upgrade Paths for 11.1.2.0.x	40
Repository Copy Paths for 11.1.2.1	40
Upgrading Checklist	41
Upgrading an Existing Data Relationship Management Application	42
Data Analysis	44
Working with External Connections	45
Data Conversion	47
Applying Updates to an Application	50
Upgrading Batch Client Scripts	50
Upgrading API Programs	50

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.

1

Installing Data Relationship Management

In This Chapter

Installation Prerequisites	7
Additional Documentation	9
About Middleware Home and EPM Oracle Home	9
Foundation Services	10
Installing Data Relationship Management	11
Troubleshooting	11

Installation Prerequisites

Items to check:

- Oracle Hyperion Data Relationship Management, Fusion Edition 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
- 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). For all database systems, you can use the Data Relationship Management Console to change the default user from DRM_DB to a different user.

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 3.5 SP1 before installing Data Relationship Management.

Windows Server 2008 Prerequisites

When installing on Microsoft Windows Server 2008, you must install .NET Framework 3.5 SP1 from the management console.

► To install .NET Framework 3.5 SP1:

- 1 Right-click the **Start Menu** and select **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 3.5.1 Features** checkbox.
- 5 Click **Next**.
- 6 Click **Install**.
- 7 Click **Close** after the installation completes.

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.

Additional Documentation

You can find Oracle Hyperion Enterprise Performance Management System installation documentation in the Oracle Documentation Library (<http://www.oracle.com/technology/documentation/epm.html>) on Oracle Technology Network. The following documentation may be useful for installing and configuring Data Relationship Management:

- *Oracle Hyperion Enterprise Performance Management System Installation Start Here*
- *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide*
- *Oracle Hyperion Enterprise Performance Management System Installation and Configuration Troubleshooting Guide*
- *Oracle Hyperion Enterprise Performance Management System Backup and Recovery Guide*
- *Oracle Hyperion Enterprise Performance Management System High Availability and Disaster Recovery Guide*
- *Oracle Hyperion Enterprise Performance Management System Security Administration 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/EPMSys11R1*. 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's Hyperion® Foundation Services to be installed when the following optional features are used:

- User authentication with external user directories such as LDAP.
- Load balancing Data Relationship Management Web applications
- Using single-sign on with Data Relationship Management
- Integrations with Oracle General Ledger for E-Business Suite and Fusion Accounting Hub
- API programs and SOA-based processes using the Data Relationship Management web service

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

- Oracle Weblogic Server
- Oracle HTTP Server
- Oracle Web Services Manager
- Oracle's Hyperion® Shared Services

Foundation Services must be installed on a Windows server where the Data Relationship Management application server component is also installed. If Foundation Services is also installed on a different machine (for example, a Linux server), the instance of Foundation Services installed on the Windows server does not need to be in a running state, but must be configured with the same Shared Services database.

For considerations and procedures to install Foundation Services, see the "Installing EPM System Products" chapter of the *Oracle Hyperion Enterprise Performance Management Installation and Configuration Guide*.

Installing Data Relationship Management

► To install Data Relationship Management:

- 1 Navigate to the directory where you downloaded the installation program and double-click **setup.exe**.
- 2 On the **Welcome** dialog box, read the license agreement and click **Next**.
- 3 Click **Next** to accept the default installation directory for Data Relationship Management files, or click **Change**, select an installation location and then click **Next**.
- 4 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
 - DRM Documentation
 - DRM Batch Client
- 5 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**.
- 6 Click **Install**.
- 7 Click **Finish**.

Note: To create and configure Data Relationship Management applications, select the option to open the configuration console.

Troubleshooting

Problem: After installing Data Relationship Management on Windows 2008 64-bit platform, you get this error when attempting to access the Web client:

HTTP Error 500.19 - Internal Server Error The requested page cannot be accessed because the related configuration data for the page is invalid.

Solution: In the IIS configuration file (C:\Windows\System32\inetsrv\config\applicationHost.config), replace the two occurrences of Deny in this section with Allow:

```
<configuration>
  <configSections>
    <sectionGroup name="system.webServer">
      <section name="handlers" overrideModeDefault="Deny" />
      <section name="modules" allowDefinition="MachineToApplication"
overrideModeDefault="Deny" />
    </sectionGroup>
  </configSections>
</configuration>
```

Problem: When Data Relationship Management is installed on IIS 7 (Windows 2008), you encounter this error message when attempting to access online help from the Data Relationship Management Web client or the Data Relationship Management migration client.

HTTP Error 4.4.0 - Not Found

Solution: Install IIS 6 Metabase Compatibility on the server:

- To install IIS 6 Metabase Compatibility:
 - 1 Click **Settings**, and then **Control Panel**.
 - 2 Select **Programs and Features**.
 - 3 Click **Turn Windows features on or off**.
 - 4 Under **Roles**, select **Web Server (IIS)**.
 - 5 Under **Role Services**, select **IIS 6 Metabase Compatibility** and click **OK**.

2

Configuring Data Relationship Management

In This Chapter

Configuring Foundation Services for Data Relationship Management	13
Configuring CSS Mode for Data Relationship Management	14
Configuring Data Relationship Management Applications	14
Configuring the Migration Utility	25
Load Balancing Data Relationship Management Web Applications	26
Using Single Sign On with Data Relationship Management	27
Terminating SSL at the Web Server	29

The Data Relationship Management Configuration Console is an application server configuration and monitoring utility.

When you install Data Relationship Management, the Data Relationship Management Console is automatically installed. You can open the console at the end of the installation program.

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

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 Hyperion Enterprise Performance Management User and Role Security Guide*.

For development purposes, Shared Services can be configured to use the WebLogic embedded LDAP server as an external directory. For information, go to: <http://www.oracle.com/>

technetwork/middleware/bi-foundation/resource-library-090986.html and select **EPM System Tips & Tricks 1-72 (PDF)**. In that document, see "Is it possible to use the WebLogic embedded LDAP server as an external directory for EPM System 11.1.2 products?".

Configuring Shared Services for Single Sign On

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

Configuring CSS Mode for Data Relationship Management

The Data Relationship Management server must be configured for CSS Authentication mode in order to authenticate users using Shared Services. See "[CSS](#)" on page 23 and "[Configuring Authentication Settings](#)" on page 24.

Configuring Data Relationship Management Applications

You can run one or more Data Relationship Management applications on a single machine. Applications can also run on multiple machines. Each application has a controller, a set of engines, and a repository connection.

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.

Caution! It is recommended that you first set up all secondary servers (servers that are not the application controller and where the Application Server and Web Server components are installed), then configure the application controller server. 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.

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

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.

Starting the Data Relationship Management Console

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

Simple Configuration Scenario

The simplest installation for Data Relationship Management is installing all components on one computer.

- To configure Data Relationship Management in the simplest scenario:
 - 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 15](#).

- 3 Click **Save Configuration**.
- 4 From the **Local Service** menu, click **Start** to start the Data Relationship Management service.

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 42](#).

- 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 selected to generate scripts in the previous step, go to [“Generating SQL Scripts” on page 18](#).
- If you select any other option in the previous step, continue to the next step.

5 Do the following:

- Select the database provider: Oracle or SqlServer.
- 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:** Change the Connection Timeout or Command Timeout.

Note: 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**.

The screenshot shows a configuration form with the following fields and values:

- Database Provider:** Oracle (selected from a dropdown)
- Service Connection:** //localhost:1521/orcl
- User ID:** sa
- Password:** *****
- Connection Timeout (Seconds):** 60 (with up/down arrows)
- Command Timeout (Seconds):** 900 (with up/down arrows)
- Test Connection:** A button with a dashed border.

Below the Service Connection field, there is a text label: `* Connection Format: [//][host_name[:port]]/service_name`

6 Click **Next**.

7 Do one of the following:

- If you selected Oracle for the database provider, continue to the next step.
- If you selected SqlServer, go to [“Creating a SQL Server Database” on page 17](#).

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**.

On the completion page, click **Save Log** 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 exits 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 there, but the settings are not applied to any application. The new database is applied when you save the configuration.

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

Creating a SQL Server Database

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

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

The screenshot shows a configuration window with two main sections: 'User Settings' and 'Repository Settings'. In 'User Settings', 'User Id' is 'DRM_DB', 'Password' is masked with '*****', and 'Confirm Password' is also masked. In 'Repository Settings', 'Database Name' is 'DRM_v1112' and 'Use server defaults for data files' is unchecked. Below this, the 'Data File' section shows 'Name' as 'DRM_v1112', 'Path' as 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data', and 'Size (Mb)' as 5. The 'Log File' section shows 'Name' as 'DRM_v112_log', 'Path' as 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data', and 'Size (Mb)' as 5.

- 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 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.
- 7 From the **Application** menu, select **Apply Updates** to initialize the repository.

Note: The Data Relationship Management service will not start properly if **Apply Updates** is not run to initialize the repository.

Configuring Host Computers

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

- [Process Manager](#)
- [Event Manager](#)
- [Engine Hosts](#)
- [API Adapter Hosts](#)
- [UI Web Servers](#)
- [CSS](#)

Note: If all components are on the same computer and you are not using Shared Services, then no additional configuration is needed. If you are using Shared Services, you must configure CSS.

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.

- To configure an optional secondary Data Relationship Management Engine Host computer:

- 1 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 Console for configuration on the secondary server.

- 2 Start the Data Relationship Management service on the secondary server.
- 3 On the application controller, under the **Engine Hosts** tab, enter the computer name of the secondary Engine Host and the maximum number of Data Relationship Management engines to be started on the host.

- 4 Save the configuration and start the Data Relationship Management service on the application controller.

When properly configured, `drm-engine.exe` processes will be launched on the application controller and secondary Engine Host computers as required by the Data Relationship Management application controller. To troubleshoot configuration issues, refer to the Windows event logs on the Data Relationship Management application controller and secondary Engine Host computers.

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.

- To configure the API Adapter Host on a secondary computer:

- 1 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 Console for configuration on the secondary server.

- 2 Start the Data Relationship Management service on the secondary server.
- 3 On the application controller, under the **API Adapter Hosts** tab, enter the secondary computer name, port number, and certification number to enable SSL.
- 4 Save the configuration and start the Data Relationship Management service on the application controller.

When properly configured, the `drm-api-adapter.exe` process will be launched on the API Adapter Host computer(s). To troubleshoot configuration issues, refer to the Windows event logs on the Data Relationship Management application controller and API Adapter Host computers.

UI Web Servers

On the UI Web Servers tab, you list the servers that are configured to run the Data Relationship Management Web client application. You can also set up anonymous profiles which allow access to the Web client via a custom URL without the user having to login.

► To configure UI 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 **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`

► To configure a secondary Data Relationship Management UI Web Server computer:

- 1 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 Console for configuration on the secondary server.

- 2 Start the Data Relationship Management service on the secondary server.
- 3 On the application controller, under the **UI Web Servers** tab, enter the name of the server(s) that are configured to run the Data Relationship Management Web client application.

- 4 Save the configuration and start the Data Relationship Management service on the application controller.

CSS

Data Relationship Management must be configured with Shared Services in order to enable external user authentication or single sign-on.

► To configure Shared Services:

- 1 On the **General** tab, configure the following options:

- **Enable CSS Bridge** – Select to enable the connection to Shared Services
 - **Enable SSO** – Select to enable Single Sign On.

Note: For information on SSO, see [“Using Single Sign On with Data Relationship Management” on page 27](#). For information on setting authentication settings, see [“Configuring Authentication Settings” on page 24](#).

- **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.
 - The CSS Bridge Host/Shared Services computer must be running a supported Microsoft Windows operating system.
 - The CSS Bridge Host/Shared Services computer can be the primary Data Relationship Management server (application controller), or a different Windows computer. It is not required to install Shared Services on the Data Relationship Management server as in releases prior to 11.1.2.
 - If the designated CSS Bridge Host is not the primary Data Relationship Management server, you must install the Data Relationship Management Application Server component on the CSS Bridge Host computer. After installation and configuration are complete, you must start the “Oracle DRM Server Processes” service on the CSS Bridge Host **before** starting the “Oracle DRM Server Processes” service on the Data Relationship Management application controller.
 - If the primary Shared Services host is not a Windows computer (for example, a UNIX server), Shared Services must be installed on a Windows computer to serve as the CSS Bridge Host and the Oracle EPM System Configurator must be run on the Windows computer to point to the Shared Services repository enabling access for the Data Relationship Management CSS Bridge. In this case, the Foundation Services service on the Windows computer does not need to be started/running.
 - When properly configured, the `drm-netjbridge-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\EPMSys11R1\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 which is not necessarily the Data Relationship Management server, which is not necessarily the Data Relationship Management 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\EPMSys11R1\products
\DataRelationshipManagement\server\jar\awbutil.jar
```

```
C:\Oracle\Middleware\EPMSys11R1\products
\DataRelationshipManagement\server\jar\cassecurity.jar
```

```
C:\Oracle\Middleware\EPMSys11R1\common\jlib\11.1.2.0\epm_j2se.jar
```

```
C:\Oracle\Middleware\wlserver_10.3\server\lib\wlsqserver.jar
```

```
C:\Oracle\Middleware\modules\javax.servlet_1.0.0.0_2-5.jar
```

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.
- 2 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.
- 3 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.

- 4 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 logins before a user is locked out.
- 5 Click **Save Settings**.

Saving Configuration Settings and Starting the Service

It is important to save configuration settings before continuing.

➤ 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**.

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.

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\EPMSys11R1\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

Key	Description
configuredServers	Specifies the admin-configured connections. Default value is <code>net.tcp://localhost:5210/Oracle/Drm/ProcessManager</code> where <i>localhost</i> is the computer and 5210 is the configured process manager port.

Key	Description
maximumExceptionsOnImport	<p>If the Continue After Error option is selected, specifies the maximum number of exceptions that can be generated during a load.</p> <p>Specify an integer greater than 0. The default value is 1000.</p>
showExceptionDetail	<p>Specifies whether detailed exception information is displayed on the error page.</p> <p>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.</p> <p>Specify True to enable exception detail or False to display detail according to the log4net settings. The default value is False.</p>
enableAboutPage	<p>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.</p> <p>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.</p> <p>Specify True to show the About page. The default value is False.</p>

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 “Oracle HTTP Server Installation Prerequisites” in the *Oracle Hyperion Enterprise Performance Management 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 [“UI Web Servers” on page 22](#).
 - 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); path=/drm-web-  
client;" env=BALANCER_ROUTE_CHANGED
```

- 7 **Add the following Forward and Reverse Proxy directives.**

```
#The actual ProxyPass  
ProxyPass /drm-web-client balancer://iisdrm stickysession=BALANCEID nofailover=Off  
  
#Do not forget ProxyPassReverse for redirects  
ProxyPassReverse /drm-web-client http://<drm_web_server1>:80/drm-web-client  
ProxyPassReverse /drm-web-client http://<drm_web_server2>:80/drm-web-client
```

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

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

Using Single Sign On with Data Relationship Management

Single Sign On (SSO) is available for users of the Data Relationship Management web client using a web access management solution (such as Oracle Access Manager). Shared Services and an external user directory (such as Oracle Internet Directory or Microsoft Active Directory) must also be set up and configured with Data Relationship Management to authenticate users using SSO.

Use the following steps to install and configure SSO:

Task	Reference
1. Configure Shared Services with an external user directory.	See “Configuring Shared Services with an External Provider” on page 13.
2. Configure Shared Services for SSO.	See “Configuring Shared Services for Single Sign On” on page 14.

Task	Reference
3. In the Data Relationship Management Configuration Console, configure Data Relationship Management for CSS authentication mode and enable SSO.	See “CSS” on page 23.
4. Configure a Web access 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 28.

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.

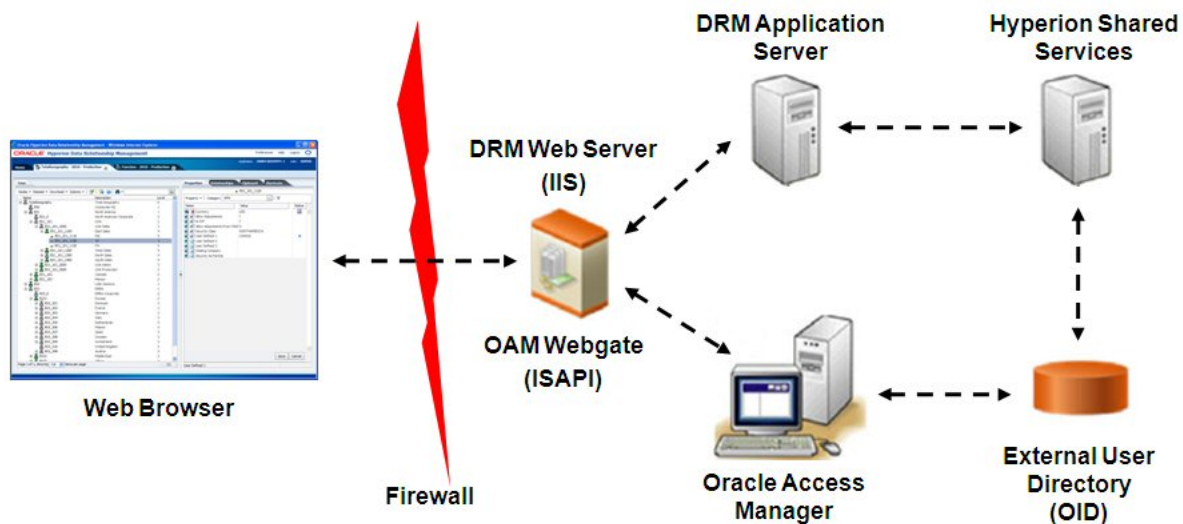
Oracle Access Manager

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, 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*.

After OAM is configured, an ISAPI filter for IIS must be installed on the server in which your Data Relationship Management Web application is running. The WebGate module intercepts HTTP requests for Web content on the server and forwards the requests to Oracle Access Server. This is the only extension that needs to be installed on the Data Relationship Management Web tier.

The component that installs that filter is the Oracle Access Manager ISAPI Webgate module. For the ISAPI Webgate module 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:



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 Hyperion Enterprise Performance Management System Security Administration Guide*.

3

Deploying and Configuring the Data Relationship Management Web Service API

In This Chapter

System Requirements	31
Deployment Prerequisites	31
Deploying the Web Service.....	33
Securing the Data Relationship Management Web Service.....	33
Testing the Data Relationship Management Web Service Using Oracle Enterprise Manager	35
Troubleshooting	36

The Data Relationship Management Web Service API provides for integration with the Data Relationship Management server. The Web service is accessed over HTTP using the SOAP protocol. It is implemented in Java and is deployed to the WebLogic application server. It communicates internally with the Data Relationship Management API Adapter service.

System Requirements

- Oracle WebLogic Server 11g
- Data Relationship Management API Adapter
- Oracle Web Services Manager (OWSM)
- Shared Services

Deployment Prerequisites

The following section includes prerequisites for deploying the Data Relationship Management Web Service API.

Installing and Configuring Foundation Services

To support Web Services (WS) Security, Shared 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's Hyperion® Foundation Services, see [“Foundation Services” on page 10](#).

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:

- “RCU Requirements for Oracle Databases” in *Oracle Fusion Middleware System Requirements and Specifications*
- “Create Schemas for Oracle SOA Suite and Oracle BAM” in *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite*

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

Configuring Oracle Web Services Manager

Configure Oracle Web Services Manager by running the Oracle Fusion Middleware Configuration Wizard to configure a WebLogic domain, and select the products that you want to configure in that domain. To start the Configuration Wizard, select the **Configuration Wizard** icon from the **Tools** menu in the **Weblogic Server** menu.

Note: EPM System and Oracle Web Services Manager must be deployed to the same domain. The choice you make for the domain depends on your deployment scenario.

➤ To configure Oracle Web Services Manager:

1 Do one of the following:

- In a new deployment, where you have not yet configured any EPM System products, create a new WebLogic domain.
- In an existing deployment, where you have already configured some EPM System products and now want to extend the deployment to include the Data Relationship Management Web service, you must extend the existing WebLogic domain created during EPM System deployment.

2 During deployment, select the following products: WSM Policy Manager, and Oracle JRF.

3 Select the default JDK. Oracle recommends that you select Production Mode.

Note: If you installed Weblogic from the Foundation Services installation, the user name and password to start the Admin Server or log into the admin console is the same user name and password entered in the EPM System Configurator for Foundation (epm_admin by default).

4 When you configure the JDBC datasources, enter the database details you entered when you ran the Repository Creation Utility (RCU).

- 5 Oracle recommends deploying the Data Relationship Management Web Service to a Managed Server instead of the AdminServer which is installed by default when you create a domain. In the **Optional Configuration** section, select **Managed Servers, Clusters and Machines** to create a Managed Server.

Configuring Weblogic with an External Provider

To configure Weblogic, see “Connecting Oracle Internet Directory (OID), Microsoft Active Directory (MSAD), or SunOne to the SOA Server” in the *Oracle Hyperion Enterprise Performance Management System Installation and Configuration 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 19.

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

The `oracle-epm-drm-webservices.ear` file should be deployed to an existing Weblogic domain.

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/technetwork/indexes/documentation/index.html#middleware>.

Securing the Data Relationship Management Web Service

It is important to protect the Data Relationship Management Web service 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 service:

Purpose	Policy
Integration with E-Business Suite General Ledger	oracle/wss_username_token_service_policy

Purpose	Policy
Integration with Oracle Fusion Accounting Hub	oracle/wss_saml_or_username_token_service_policy
Workflow Development Kit or custom API programs	One or more of the following: <ul style="list-style-type: none"> ● oracle/wss11_saml_or_username_token_with_message_protection_service_policy ● oracle/wss_username_token_service_policy ● oracle/wss_saml_or_username_token_service_policy

For more information, see “Attaching Policies to Web Services” in *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

Configuring Policies in Oracle Web Services Manager

To configure policies for the Data Relationship Management Web Service in Oracle Web Services Manager, see "Configuring Policies" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

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.

► To configure the Data Relationship Management API Adapter for SSL:

1 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 that does not include message protection. 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.

Note: After changing the security policy, you may need to restart the Weblogic target server to which the Data Relationship Management Web Service is deployed.

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

For example: `http://localhost:28080/oracle-epm-drm-webservices/DrmService?wsdl`
- 4 From **Operation**, select an operation; for example `getSysPrefs`.
- 5 On the **Request** tab, select **WSS Username Token** and enter a username and password with which to authenticate.

Note: The user must exist in the security realm for the Weblogic domain and in Shared Services.

- 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.

```
<soap:Header>
<AppParameters xmlns="http://drm.webservices.epm.oracle">
<serverUrl xmlns="http://drm.webservices.epm.oracle">http://localhost:5240/Oracle/
Drm/APIAdapter</serverUrl>
<sessionParams xmlns="http://drm.webservices.epm.oracle">ProductVersion=11.1.
2,CultureName=en-US,TimeZoneOffset=-360</sessionParams>
</AppParameters>
</soap:Header>
```

Note: Required parameters must be populated for Data Relationship Management operations otherwise an error occurs.

- In the soap header argument in step 6, modify the `serverUrl` to the appropriate value for the Data Relationship Management API adapter.
- Click **Test Web Service**.

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

- After testing is complete, re-attach the required production policy: `oracle/wss11_saml_or_username_token_with_message_protection_service_policy`

Troubleshooting

Error	Possible Cause	Recommendation
Oracle EPM Foundation Agent Error in request: begin session (message: Cannot begin session. EPMCSS-00301: Failed to authenticate user. Invalid credentials. Enter valid credentials.	Shared Services doesn't contain the user identity.	Ensure Data Relationship Management is configured with the same User directory as used by the Weblogic realm.
javax.xml.ws.soap.SOAPFaultException: FailedAuthentication : The security token cannot be authenticated.	User identity is not present in Weblogic security realm.	Configure the Weblogic Realm with the appropriate authentication provider for the realm. Ensure that it is configured to point to the same provider with which Shared Services is configured.

Error	Possible Cause	Recommendation
javax.xml.ws.WebServiceException: Failed to access the WSDL at: http://localhost:7001/oracle-epm-drm-webservices/DrmService?WSDL.	Host or port is incorrect. The Web service is not running on the Weblogic domain.	Verify the Data Relationship Management Web service is deployed and running on the Weblogic domain. Modify the host/port reference in the WSDL URL.
Error while trying to communicate with DRM API Adapter at: http://localhost:5240/Oracle/Drm/APIAdapter/.	Host or port is incorrect. The API adapter is not running or configured correctly.	Verify the API adapter is configured and running. Change the API adapter URL in the client program/application to the correct value.
javax.xml.ws.soap.SOAPFaultException: SOAP must understand error:{http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd}Security, {http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd}Security.	No OWSM policy is attached to the Data Relationship Management Web service or, if a policy exists, the policy is disabled. OWSM is not configured correctly and is not functioning. Ensure that the servlet can be reached and that the Policy Manager Status is "Operational" http://<host>:<port>/wsm-pm/validator	Attach either a global or local policy to the Data Relationship Management Web service. Follow the steps in the OWSM troubleshooting section: http://download.oracle.com/docs/cd/E12839_01/web.1111/b32511/diagnosing.htm#CHDIDCHA

4

Upgrading a Data Relationship Management Installation

In This Chapter

Supported Upgrade Paths	39
Upgrading Checklist	41
Upgrading an Existing Data Relationship Management Application	42
Applying Updates to an Application	50
Upgrading Batch Client Scripts	50
Upgrading API Programs	50

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.

Supported Upgrade Paths

You can upgrade to Data Relationship Management Release 11.1.2.1 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 prior to 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. Additionally, the wizard provides the ability to copy a repository from a current release to a different repository running on the same or a different database provider.

Note: The following sections describe the high-level options for upgrading or copying a repository. For detailed instructions, see [“Upgrading an Existing Data Relationship Management Application”](#) on page 42.

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.
 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

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

Caution! You cannot upgrade an 11.1.2.0.x repository to an existing, new repository. You will receive an error such as: *DRM-79842: Source data model version 11.1.2.0.1.1 and target data model version 11.1.2.1.0.32 do not match. Direct copy is not possible between databases unless the data models exactly match.*

- Upgrade path option 2:
 1. Create a new application and specify the repository connection information for an existing 11.1.2.0.x repository.
 2. Run the **Apply Updates** utility.

Repository Copy Paths for 11.1.2.1

- 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.
 2. Run the **Copy or Upgrade an Existing Repository** option using the new repository created in step 1 as the target connection.

Upgrading Checklist

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

Table 2 Upgrading Checklist

Task	Reference
<p>1. Review release compatibility, system requirements, and other prerequisites for this release.</p> <p>If your database environment needs to be upgraded, perform the database upgrade before you proceed. See the database documentation for details.</p> <p>Note: If you are using Shared Services, you must upgrade the Oracle's Hyperion® Shared Services installation before upgrading the Data Relationship Management. For more information, see the <i>Oracle Hyperion Enterprise Performance Management System Installation and Configuration Guide</i>.</p>	<ul style="list-style-type: none"> ● “Installation Prerequisites” on page 7 ● <i>Oracle Hyperion Enterprise Performance Management System Certification Matrix</i> (http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html) ● <i>Oracle Hyperion Enterprise Performance Management System Installation Start Here</i>
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.
3. Download and prepare the installation files.	Download files for Release 11.1.2.1 and extract the zip file contents.
4. Stop Data Relationship Management services.	If you are installing Release 11.1.2.1 on the same machine as the earlier release installation, stop the Data Relationship Management services.
5. Uninstall the earlier release of Data Relationship Management.	<p>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.</p> <p>If you are upgrading from a release prior to 11.1.2, you must first manually uninstall the old release and then install the new release.</p>
6. Install release 11.1.2.1 of Data Relationship Management	“Installing Data Relationship Management” on page 11.
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 42.
8. Undeploy the 11.1.2 Web Service.	If upgrading the Web service from 11.1.2, the Web service DrmWebService can be undeployed using the Weblogic console. Instructions on how to undeploy a Web service can be found in the <i>Oracle Fusion Middleware Security and Administrator's Guide for Web Services</i> .
9. Optional: Deploy and configure the Web Service.	Chapter 3, “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 release 9.2.x, 9.3.x, and 11.1.x and copy applications from the current release.

Note: For release-specific upgrading and copying information, see [“Repository Upgrade Paths for 9.2.x, 9.3.x, and 11.1.1.x” on page 40](#), [“Repository Upgrade Paths for 11.1.2.0.x” on page 40](#), and [“Repository Copy Paths for 11.1.2.1” on page 40](#).

► 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.

- 3 On the **Repository Configuration** tab, click the **Repository Wizard** button.
- 4 On the **Select the Desired Repository Operation** page, 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 SqlServer.
 - 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:** Change the Connection Timeout or Command Timeout.
 - e. Click **Test Connection**.
- 6 Click **Next**.
- 7 On the **Target Connection** page, do the following:
 - Select the database provider: Oracle or SqlServer.
 - 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:** Change the Connection Timeout or Command Timeout.

Note: 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**.

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 44](#) and [“Data Conversion” on page 47](#).

10 Click **Next**.

11 Do one of the following:

- If you selected Oracle for the database provider, continue to the next step.
- If you selected SqlServer, go to [“Creating a SQL Server Database” on page 17](#).

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**.

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.

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**.

On the completion page, click **Save Log** 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” on page 19](#)
- [“Configuring Authentication Settings” on page 24](#)
- [“Saving Configuration Settings and Starting the Service” on page 25](#)

Data Analysis

The Repository Analysis page provides information about the source database so that decisions can be made that affect size and objects in the new database. 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 database. Sizing found here is automatically applied to the Repository User and Data File settings page. 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 45](#).
- **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 45](#).
- **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 45](#).

- **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 scenarios, during repository analysis, the property definition is flagged and the record is **not** copied to the upgraded database.

- A global property that has been referenced in Property_Local table as a local property
- A local property that has been referenced in Property_Global table as a global property


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.



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 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 46](#).

► 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

If an ADMIN user exists in the source system, the password is reset to the password specified in the upgrade process. 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.

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

Old User Type	Assigned Functional Roles
System	Access Manager Application Administrator Data Manager Workflow User
Functional	Data Manager Workflow User
Security	Access Manager
User	Interactive User Workflow User

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 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 dates are converted using the offset dictated by the time zone in which the console is running, regardless of when the date falls. 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 upgrade purposes, dates are converted using the standard offset. For all new data added after the repository is upgraded, the stored dates 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:

Old Transaction Name	New Transaction Name
Automator Run	Action Script Run
Migration Extract	Migration Export
Migration Load	Migration Import
Add System Category	Admin Add Hierarchy Group
Update System Category	Admin Update Hierarchy Group
Delete System Category	Admin Delete Hierarchy Group

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.

Applying Updates to an Application

- To apply updates to an existing 11.1.2.0.x repository:
 - 1 Create a new application.
 - 2 On the **Repository Configuration** tab, specify repository connection information for an existing 11.1.2.0.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.

Upgrading Batch Client Scripts

To function properly, Batch Client scripts from releases prior to 11.1.2 must be manually upgraded. You must make the following 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).

Documentation for additional Batch Client parameters for new features can be found in the *Oracle Hyperion Data Relationship Management User Guide*.

Upgrading API Programs

API programs used with Oracle Hyperion Data Relationship Management, Fusion Edition releases prior to 11.1.2.1 must be manually upgraded to use the Web service API offered in this release. Enhancements to the Web service API are covered in the *Oracle Hyperion Data Relationship Management New Features Guide*. For more information on the Web service API, see the *Oracle Hyperion Data Relationship Management API Guide*.