Oracle® Universal Content Management

UCM-IRM Integration Guide

Release 10*g*R3

September 2008

ORACLE®

UCM-IRM Integration Guide, Release 10*g*R3

Primary Author: Matt Hoffman

Contributing Authors: Sandra Christiansen, Martin Wykes

Contributor: Blair Butterworth

Contents

Preface

This guide addresses the installation and configuration of Oracle UCM-IRM integration components on Oracle Content Server and Inbound Refinery.

Audience

This document is intended for administrators who will install the Oracle UCM-IRM integration components on Oracle Content Server and Inbound Refinery.

The audience for this guide is assumed to have advanced knowledge of Oracle Content Server and its configuration. Familiarity with Oracle IRM Server and its configuration is also assumed.

> **Important:** It is assumed that the person doing the installation has sufficient rights and permissions on both Oracle IRM Server and Oracle Content Server. Failure to secure the proper rights and permissions will negatively affect the installation process.

Related Documents

For more information, see the following documents in the Oracle IRM 10g Release 3 documentation set:

- Oracle IRM Server Online Help
- Oracle IRM Server Installation Guide
- Oracle IRM Management Console Installation Guide

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Convention	Meaning
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

The following presentational conventions are used throughout this guide:

- Forward slashes (/) are used to separate parts of an Internet address. For example, `http://www.google.com/maps`. A forward slash might or might not appear at the end of an Internet address.
- Backward slashes (\) are used to separate the levels in a path to a Microsoft Windows server, directory, or file. For example, C:\ibr\refinery\. A backward slash will always appear after the end of a Microsoft Windows server, directory, or file path. For UNIX/Linux, reverse the slash direction.
- File names and file paths within text are indicated by the following convention: <*filename*> file in the <*path_to_directory*> directory.
- The notations <*content_server_install_dir*>, <*cs_install_dir*>, <*install_dir*> are used to refer to the location of the main Oracle Content Server installation directory.

1

UCM-IRM Integration Overview

The purpose of UCM-IRM integration is to allow content processed by Oracle Content Server to have the security protection offered by Oracle IRM.

This section covers the following topics:

1.1 About Oracle IRM

Oracle IRM uses encryption to “seal” content, ensuring that only authorized persons can use it.

Oracle IRM enables organizations to:

- Retain control of sensitive information, even after it has been shared.
- Track content forwarded to internal and external audiences.
- Prevent unauthorized access to, extraction from, or editing of information.
- Revoke information access when business requirements dictate.

The key Oracle IRM components in the UCM-IRM integration are Oracle IRM Server and its associated Management Console. Oracle IRM Server stores the decryption keys and rights governing end user access to content, and the Management Console permits administrators to manage all aspects of content security.

1.2 About UCM-IRM Integration

Oracle IRM enables the sealing of content based on permissions and contexts, and the searching of content sealed in this way. When integrating with Oracle Content Server, sealing can be achieved by any method that sets the value of the IRMProtection metadata field, which is specifically added to Oracle Content Server for this purpose. Some example ways to achieve this:

- A profile called "Finance_Confidential" could set the value of the IRMProtection metadata field to "Finance_Confidential" for every document checked in using that profile, and would seal such documents to an Oracle IRM context named "Finance_Confidential".
- A global rule could derive the value of the IRMProtection metadata field based on a user’s choice of Security Group on check-in. When a user checks in a document

to the "Finance_Confidential" security group, the value of the IRMProtection field would be set to "Finance_Confidential" and the document would be sealed to an Oracle IRM context named "Finance_Confidential".

- A "global" rule could derive the value of the IRMProtection metadata field based on a logical combination of Security group and Account. Thus, if a user checks in a document for the "Finance" security group and the "Europe" account, the derived IRMProtection field could be "Finance_Europe" and, upon check-in to Oracle Content Server, the document could be automatically sealed to an Oracle IRM context named "Finance_Europe".
- An Oracle Content Server folder named "Finance_Confidential" could have default check-in values that set the IRMProtection metadata field to "Finance_Confidential", so that any document entered into the system via the Oracle Content Server Folders component would be automatically sealed to an Oracle IRM context named "Finance_Confidential".

1.3 Overview of UCM-IRM Integration Installation Procedures

UCM-IRM integration requires the following:

- Installation of Oracle Content Server (this is described in the Oracle Content Server documentation).
- Installation, enabling, and set up of the File Store Provider component of Oracle Universal Content Management. The File Store Provider Installation and Administration Guide is available from the Oracle Technology Network.
- Installation of Oracle IRM Server (this is described in the Oracle IRM Server documentation).
- Configuration of Oracle IRM Server. This is described in this guide in Chapter 2, "Configuring Oracle IRM Server for UCM-IRM Integration", and is summarized below:
  - Creation of a special user for use with Oracle Content Server.
  - Creation of two or more Oracle IRM contexts.
  - Creating of Oracle IRM roles, and assignment to Oracle IRM contexts. **It is important to name the roles exactly as specified in the instructions, otherwise integration will fail.**
  - Copying of user information from Oracle Content Server to Oracle IRM Server.
- Installation of the two UCM-IRM integration components:
  - UCM-IRM Integration IDC component (installed in Oracle Content Server)
  - UCM-IRM Integration IBR component (installed in the Inbound Refinery product)

  Installation of these components is described in this guide in Chapter 3, "Installing the UCM-IRM Integration Components"
- Configuration of Oracle Content Server. This is described in this guide in Chapter 4, "Configuring Oracle Content Server for UCM-IRM Integration".
- If required, IIS Web Server configuration and the enabling of icons for sealed documents. These are described in this guide in Chapter 4, "Configuring Oracle Content Server for UCM-IRM Integration".
- Assigning of roles to end-users (through Oracle IRM groups) in Oracle IRM Server, to allow users to open and work with content. These role assignments are critical

to creating a useful system that enforces desirable security policy while allowing valid workflows to be performed.

2

Configuring Oracle IRM Server for UCM-IRM Integration

The information in this section contains the procedures necessary to configure Oracle IRM Server to interface with Oracle Content Server.

This section covers the following topics:

2.1 Oracle IRM Server Configuration

Before installing UCM-IRM integration components on Oracle Content Server and Inbound Refinery, you must first configure Oracle IRM Server to interface with Oracle Content Server.

This setup includes enabling web services, creating a special user with the proper rights, creating roles for Oracle Content Server users, creating the Oracle IRM contexts for sealed documents, and importing the Oracle Content Server user list.

2.1.1 Enabling Web Services

By default, Web Services are disabled in Oracle IRM Server.

Use the following procedure to enable Web Services in Oracle IRM Server.

1. In the Microsoft Windows operating system, stop the Oracle IRM Server service. The service name is "Oracle Information Rights Management Server".
2. Open the server.properties file. This file is located under the installation directory. The default location is as follows:

```
%ProgramFiles%\Oracle\Information Rights Management\ls\properties\server.properties
```

3. Locate the configuration setting called sealedmedia.server.plugins.

   ```
   sealedmedia.server.plugins =
   ```

   Append to the end of the setting the location of the Oracle IRM Server Web Services plugin. This file is installed with Oracle IRM Server.

   ```
   sealedmedia.server.plugins=[existing settings],c:\\Program
   Files\\Oracle\\Information Rights Management\\ls\\bin\\smsoapp.dll
   ```

   Note the use of the comma (,) to delimit plugin DLLs and the use of double backslashes.

4. Save the file.
5. Restart the Oracle IRM Server service.

   To confirm the Web Services are enabled, open a browser and navigate to http://localhost/sm/wsdl/oracleirm.wsdl

   The browser should download/display the Oracle IRM Server WSDL document.

2.1.2 Creating the Special User UCM-IRM.user

You need to create a special Oracle IRM user (UCM-IRM user) to act on behalf of the Oracle Content Server system.

Use the following procedure to create the special user:

1. Start the Oracle IRM Management Console.
2. Log in to Oracle IRM Server as an administrator, with "Owner" rights and permissions.
3. In the Management Console, select **IRM Servers**, then select **Oracle IRM Server**, then select **Users and Groups**.
4. Click **New User**, and enter the user name in the text box. Name the user "UCM-IRM.user". This name will appear in the sealed document properties as the user that initially sealed that document.
5. Click **Next**.
6. Select **Standard authentication**, and then click **Next**

   Note: Windows authentication is not supported.

7. Enter and confirm the password. Do not set the password settings to require the user to change password at the next login, or disable the user from resetting the password. Click **Next**.
8. Enter optional details (first name, last name, or email), and click **Finish**.

2.1.3 Creating an Oracle IRM Context Template

It is necessary to create an Oracle IRM context template for the special user (UCM-IRM user) created in the previous section. This context template must include the minimum set of rights needed for UCM-IRM integration to perform all its actions. This single context template is the basis from which all other Oracle IRM contexts will be derived. It will be copied and altered as necessary for the rest of the contexts needed during the deployment of the UCM-IRM integration.

Use the following procedure to create an Oracle IRM context template:

1. In the Oracle IRM Management Console, select **IRM Servers**, then select **Oracle IRM Server**, then select **Contexts**.
2. Click **New Context**. Enter a name and a brief description for the new context. The context name should be descriptive for the types of information being sealed, for example “Internal_Only”. (See the Oracle IRM Server documentation guidance on context naming.) Click **Next**.
3. You are prompted for values for the Information URL, Oracle IRM Server and Compatibility Desktop Software. Click **Next** after you enter each value.

   The newly created context is displayed in the Oracle IRM Contexts folder.

2.1.4 Assigning Roles to the Context Template

Once the context template has been created, you must create a set of two administrator and one non-administrator roles and assign them to the UCM-IRM user (the special user created previously).

Use the following procedure to create the roles for the Oracle IRM context template:

1. Start the Oracle IRM Management Console.
2. Log in to Oracle IRM Server as an administrator, with "Owner" rights and permissions.
3. In the Management Console, select **Administrators**, then select **Roles**. Click **New Role**.
4. In the New Administrator Role screen, name the role "UCM-IRM integration". (Using another name will cause integration to fail.) Add a description of the role, and click **Next**.
5. Set the Access Settings as desired, and click **Next**.
6. In the Select Operations screen, toggle from the task list to the methods list. Select and add the following methods:
   - AdminAPI.GetServerSettings
   - RoleAPI.ListRightsByAccount
   - ContextAPI.ContextExists
   - ContextSealingServices.ListResealableContext
   - SealingServices.ListSealableTypes
7. Click **OK**, and then click **Finish**.
8. Assign the role created above to the UCM-IRM user.
9. Create an administrator role in the newly created context template, and name the role "UCM-IRM integration". (Using another name will cause integration to fail.) Add the following operations:
   - SealingServices.SealContent
   - UnsealingServices.UnsealBytes
10. Assign the role created in the previous step to the UCM-IRM user.
11. Create a standard role (that is, not an administrator role) in the newly created template context, name the role "UCM-IRM integration" (using another name will cause integration to fail), and add the following features:
    - Reseal

- Seal

12. Assign the role created in the previous step to the UCM-IRM user.

2.1.5 Designing the Context Model

It is important to consider the contexts that you need to create, based on a mapping model linking Oracle IRM contexts to an entity in the Oracle Content Server system, for example, Security Groups. Remember to insure that you provide your users with the appropriate Oracle IRM context to seal their content at check-in.

For an example of a simple mapping model, see Section 2.2.4, "Security Synchronization between Oracle Content Server and Oracle IRM Server".

Once the model is defined you can copy and rename the context template created in Section 2.1.3, "Creating an Oracle IRM Context Template".

2.2 User Creation

This section provides information on how to create users manually or automatically, depending on your requirements.

2.2.1 Introduction

Oracle Content Server users need accounts in Oracle IRM Server to open or save sealed documents. Users can be created in Oracle IRM Server in two ways: manually or automatically. For a smaller number of users, this process is best done manually. If the system contains a larger number of users, it is best to employ Oracle IRM Gateway to automatically import users, either from an LDAP directory or from the Oracle Content Server database, using Oracle Virtual Directory, into Oracle IRM Server.

2.2.2 Manual User Creation

For a small number of users, user creation is best achieved manually via the Oracle IRM Management Console. Use the following procedure to create individual users from the Oracle IRM Management Console:

1. Start the Oracle IRM Management Console.
2. Log in to Oracle IRM Server as an administrator, with "Owner" rights and permissions.
3. In the Management Console, select **IRM Servers**, then select the name of the Oracle IRM Server instance, then select **Users and Groups**.
4. Click **New User**, and enter a user name in the text box. This name will appear in the properties for a sealed document as the user that sealed that document.
5. Click **Next**.
6. Select **Standard authentication**, and then click **Next**

> **Note:** Windows authentication is not supported.

7. Enter and confirm the password. Do not set the password settings to require the user to change password at the next login, or disable the user from resetting the password. Click **Next**.
8. Enter an email address, for later possible use with the password reset facility.

9. Enter optional details (first name, last name) and click **Finish**.

2.2.3 Automatic User Creation

There are two main ways in which users can be created in Oracle IRM Server automatically:

- Oracle IRM Gateway can be used to extract user information from LDAP directories (such as Oracle Virtual Directory, Active Directory, and Sun ONE Directory). See the Oracle IRM Gateway documentation for how to do this.
- The Oracle Virtual Directory Server and Management application can be used to import large numbers of users from the Oracle Content Server to Oracle IRM Server. This method is described below.

Use the following procedure to import Oracle Content Server users into Oracle IRM Server using the Oracle Virtual Directory Server and Management application:

1. Install and configure the Oracle Virtual Directory Server and Management application in accordance with its documentation. Start the application.
2. Click **File** then select **New** and then **Directory Management Project**. Give it a descriptive name, and then click **Finish**.
3. Right-click the new project, click **New**, then select **Virtual Directory Server**.
4. Name the server, then modify the IP address to the address of the machine containing the installed Oracle IRM Server. Enter the password, and click **Verify SSL**. Click **Finish**.
5. Download the JDBC drivers for the type and version of the database used by the Oracle Content Server.
6. Right click the newly created server, select **Manage**, then select **Server Libraries**.
7. Click **Select New**, browse to the location of the drivers you downloaded, and click **Open**. Once all the drivers required have been added, click **Deploy**.
8. Right-click the Adapters node in your server and select **New**, then select **Database Adapter**.
9. Enter an Adapter Name. Under Type, select the type of database used by the Oracle Content Server. Enter the IP Address of the Oracle Content Server (UCM) database under **Host**. Enter the name of the DB under Database. Enter the user credentials used to access the ACME's database.
10. Click **Validate Connection**, and once successful, click **Finish**.
11. Click the Engine node in your server, and double-click **Schema**.
12. Click **Add Object Class**.
13. Create two Object classes with the following information:
    - Object Class One
      - Name: IRMGroup
      - OID: <Any Unique String> for example, OVD-IRM_IRMGroup
      - Add the following **Required Attributes**: cn, member, name
    - Object Class two
      - Name: IRMUser
      - OID: <Any Unique String> for example, OVD-IRM_IRMUser

- Add the following **Required Attributes**: cn, givenName, mail, uid

14. Click the Adapters node in your server, and double-click the adapter you created earlier.
15. Scroll to the bottom of the information page, and click DB Attribute Mapping Wizard.
16. From the top node and using the arrow buttons located in the middle columns, select the tables USERS and USERSECURITYATTRIBUTES. Click **Next**.
17. In Table 1 select the USERS table and then select Field DNAME. In Table 2 select the USERSECURITYATTRIBUTES table, then select Field DUSERNAME. Click **Add**, then click **Next**.
18. Select the root node under Object Classes, and click **Add**.
19. Select the IRMUser Object Class, and enter cn into the RDN field. Click **OK**.
20. Click the cn - IRMUser node, then click **Add** in the Attributes panel. Enter the following:

Table 2–1

LDAP Attribute	Table	Field
Cn	USERS	DNAME
givenName	USERS	DFULLNAME
mail	USERS	DEMAIL
uid	USERS	DNAME

21. Select the root node, and click **Add**.
22. Select the IRMGroup Object Class, and enter cn into the RDN field. Click **OK**. Enter the following:

Table 2–2

LDAP Attribute	Table	Field
cn	USERSECURITYATTRIBUTES	DATTRIBUTENAME
member	USERSECURITYATTRIBUTES	DUSERNAME
name	USERSECURITYATTRIBUTES	DATTRIBUTENAME

23. Click **Finish**.
24. Right-click the server, and **Save All To Server**.
25. Ensure each alteration is uploaded to the server, and that each component then restarts.
26. Open Oracle IRM Gateway and follow the on-screen instructions, entering one of the following jobs depending on your current needs.
    - Save Users to Server
    - Save Groups to Server
    - Save Users and Groups to Server

2.2.4 Security Synchronization between Oracle Content Server and Oracle IRM Server

The following is a recommended mapping model that could be used to synchronize Oracle Content Server (UCM) users, roles and security groups with Oracle IRM users, groups and contexts.

Table 2–3

UCM	IRM	Notes
User	User	Create one IRM user for each UCM user, with identical username, full name, and email attributes.
Role	Group	Create one IRM group for every UCM role. The IRM group will contain the same set of members as the UCM role.
Security Group	Context	Create one IRM Context for the UCM Security Group.
Security Group + Account	Context	Create one IRM Context for the UCM Security Group Account combination.
Security Group + Account + Permission Level	Group	Create one Group for each unique combination of Security Group, Account and Permission Level. There are four permission levels: Read, Write, Delete and Admin.

Note: Enforcing on the Oracle IRM client a security model that was designed for server-side security is likely to lead to problems, as it might prevent previously possible and desirable workflows. If in doubt, consult with your Oracle IRM representative to help decide on a mapping model that is most appropriate for your organisation.

2.2.5 Security Considerations

After UCM-IRM integration, it remains possible to search sealed content both through metadata-based search and through text-based search (for example using the text search systems produced by Verity).

When a full text search mechanism is used, a binary replica of each document to be indexed is stored in the associated database. The database then uses its own internal indexing process to index this document. However, the document is not deleted. This potential security flaw allows anyone with access to the database to read the unsealed content of every 'Secured' document.

You can stop the unsealing of files prior to indexing, so that no unsealed content is stored. The way to do this is to uncheck the "Index Sealed File Content" option on the Oracle IRM Integration Administration page. Users may also use standard UCM methods to disable full text search.

3

Installing the UCM-IRM Integration Components

This section covers the following topics:

3.1 Pre-Installation Tasks and Considerations

Make sure that you read, understand, and comply with each of the following tasks and considerations before installing the UCM-IRM integration components on Oracle Content Server or Inbound Refinery:

- The UCM-IRM integration components can be installed on all supported Oracle Content Server and Inbound Refinery platforms.
- Oracle IRM version 10gR3 (10.1.3.3.3) requires Oracle Content Server 10g Release 3 (10.1.3.3.3) or later 10*g*R3 versions.
- The File Store Provider component of Oracle Universal Content Management must be installed before using the integration. The File Store Provider Installation and Administration Guide is available from the Oracle Technology Network.
- UCM-IRM integration requires that an Oracle Content Server user be created on the Oracle IRM Server. The user must have specific rights assigned and various contexts defined. The Oracle IRM Server Administrator must provide the path to the Oracle IRM Server, the user id, password, and context information to the Oracle Content Server Administrator, to coordinate the integration.
- Due to the technical nature of operating systems, web servers, and browsers, Oracle, Inc. cannot warrant compatibility with all versions and features of third-party products.

3.2 Installing the UCM-IRM Integration Components

The UCM-IRM integration solution uses two separate components. One component is installed on Oracle Content Server and the other on the Inbound Refinery product. The two components are:

- UCM-IRM Integration IDC (Content Server)
- UCM-IRM Integration IBR (Inbound Refinery)

Order of installation is of no consequence. These components are used in conjunction with Oracle IRM Server and the Oracle IRM Desktop application to enable the sealing and unsealing of content managed by Oracle Content Server.

Important: It is imperative that the UCM-IRM integration components are installed properly on their respective Oracle Content Server and Inbound Refinery instances (that is, the UCM-IRM Integration IBR component must be installed on Inbound Refinery, not on Oracle Content Server). Should a reversal of the components occur, the UCM-IRM integration will not work.

This section covers the following topics:

3.2.1 Installing UCM-IRM Integration Components Using Component Manager

Use the following procedure, to install the UCM-IRM integration components using Component Manager:

1. Open a new browser window, and log in to Oracle Content Server as a system administrator.
2. Launch the Admin Server.
3. On the Content Admin Server page, click the button of the content server on which to install the IRMIntegration component. The status page for the content server is displayed.
4. In the option list for the content server, click the **Component Manager** link.

   The Component Manager page is displayed.
5. Click the **Browse** button next to the **Install New Component** field.
6. Navigate to the IRMIntegration component on the content server distribution media (*UCM-IRM Integration IDC.zip*) select it, and close the file selection dialog.
7. Double-click the component zip file or select the component zip file, and click **Open**.
8. Click **Install**. An overview page is displayed providing a list of the items that will be installed.
9. Click **Continue**. All required files are now installed. This might take a few minutes.
10. After all files have been copied, a message is displayed stating that the component was uploaded and installed successfully.
11. Click the link to enable the component.

    The status page for the content server is displayed.
12. Click the restart button to restart the content server.
13. Restart the web server.

14. From the Configuration Manager, select the IRMProtection field, and click **Update Database Design**.

    To install the UCM-IRM Integration IBR component, complete the previous steps, installing instead the UCM-IRM Integration IBR component on Inbound Refinery.

3.2.2 Installing the UCM-IRM Integration Components Using Component Wizard

Use the following procedure to install the UCM-IRM integration components using Component Wizard:

1. Start Component Wizard:
   - In Windows, choose **Programs** from the **Start** menu. Then select **Content Server**, then **<*cserver*>**, then **Utilities**, and then select **Component Wizard**.

   The Component Wizard main screen and the Component List screen are displayed.
   - For content servers hosted on UNIX, navigate to the <*install_dir*>/bin directory. At the command prompt, type Component Wizard.
2. Click **Install**. The Install dialog is displayed.
3. Click **Select** and navigate to the component on the Oracle IRM distribution media (*UCM-IRM Integration IDC.zip*).
4. Double-click the zip file, or click **Open**. The Install list displays the files that will be installed.
5. Click **Continue**. All required files will now be installed: this might take a few minutes.

   The Install Settings Screen is displayed
6. After all files have been copied, you are prompted to confirm enabling the component. Click **Yes**.
7. Close Component Wizard.
8. From the Admin page, restart the content server.
9. From the Configuration Manager, select the IRMProtection field, and click **Update Database Design**.

   To install the UCM-IRM Integration IBR component, complete the previous steps, installing instead the UCM-IRM Integration IBR component on Inbound Refinery.

3.3 Uninstalling the UCM-IRM Integration Components

Use the following procedure to uninstall the UCM-IRM integration components:

1. Disable and uninstall the components using either Component Manager or Component Wizard.
2. From the Admin page, restart the content server.
3. Restart the web servers.
4. If desired, delete the following directories that were created for the UCM-IRM Integration components:
   - <*refinery_install_dir*>/custom/UCM-IRM Integration IBR
   - <*content_server_install_dir*>/custom/UCM-IRM Integration IDC

4

Configuring Oracle Content Server for UCM-IRM Integration

This section contains the procedures necessary to configure the UCM-IRM integration components.

This section covers the following topics:.

4.1 Enabling UCM-IRM Integration in Oracle Content Server

After installing the UCM-IRM integration components, you must enable the interface between Oracle IRM Server and Oracle Content Server.

The installation created an Oracle IRM Integration Administration page for Oracle Content Server. This page is used to configure and administer Oracle IRM on Oracle Content Server.

The UCM-IRM integration element on Inbound Refinery is a static installation, and no configuration is needed.

4.1.1 Opening the Oracle IRM Integration Administration Page

The connection to Oracle IRM Server is managed in Oracle Content Server using the Oracle IRM Integration Administration page.

Use the following procedure to make changes:

1. Make sure you are logged into Oracle Content Server as an administrator.
2. In the navigation menu, select **Administration**, then select **IRM Administration**.

   The "Oracle IRM Integration Administration Page" on page A-1 is displayed.

4.1.2 Oracle IRM Server and General Configuration Settings

On the Oracle IRM Integration Administration page, you enter server configuration information and specify general configuration settings.

Use the following procedure to define server configuration information for Oracle IRM Server:

1. In the Server Address text box, enter the URL or IP address of the license server (that is, the Oracle IRM Server instance). The path to the license server should take the following form:

   `http://<serverhostname>:<portnumber>/sm/sealedmedia/wsdl`

   where <serverhostname> is the hostname of the license server and <portnumber> is its port number. The port number is assumed to be 80 if not specified.

2. In the Account Username field, enter the username for the content server (that is, the Oracle Content Server instance). This must have been previously defined in Oracle IRM Server using the Oracle IRM Management Console. See "Creating an Oracle IRM Context Template" on page 2-2 for details.

3. In the Account Password field, enter the password for the Oracle Content Server account on the license server (that is, the Oracle IRM Server instance).

4. Click **Update** to apply the server configuration information.

Use the following procedure to define the general configuration information for Oracle IRM Server:

1. If required, check the box to enable the Index Sealed File Contents option.

2. If required, check the box to enable the Seal Zipped Web Renditions option.

3. Click **Update** to apply the general configuration information.

4.1.3 Defining Contexts in Oracle Content Server

Contexts have been set up for Oracle Content Server in Oracle IRM Server. See "Creating an Oracle IRM Context Template" on page 2-2 for details. These contexts must be defined in Oracle Content Server to allow the proper level of sealing of content.

Use the following procedure to define the contexts in Oracle Content Server:

1. Log in to Oracle Content Server and, from the Administration folder, select **Admin Applets**.

2. Select **Configuration Manager**.

3. Select the **Information Fields** tab, then select the **IRMProtection** field.

4. Click **Edit Tree**. The Option List screen is displayed.

5. Enter the contexts that were previously defined in Oracle IRM Server. These should be entered exactly as previously defined ("string-exact"), for current and future compatibility with the underlying database.

6. Click **OK,** and log out of the Configuration Manager.

4.1.4 IRM File Extensions for IIS

If Internet Information Services (IIS) is used as the web server for Oracle Content Server, you must add the sealed file extensions and mime types to its mime type list. If these extensions are not added, the sealed files will not open from Oracle Content Server; instead, a "404 Page not found" link will be displayed. For a list of the IIS file extension and mime types, see "IIS File Extensions for UCM-IRM Integration" on page A-2.

4.1.5 Enabling Icons for Sealed File Types

Icons are provided for sealed file types for use in customized search result templates or the Oracle Content Server interface. The deployment team should follow Oracle Content Server documentation about customization.

The path to the icons that are used to represent sealed items is defined in a variable for Oracle Content Server, called $iconPath.

Use the following procedure to enable the icons for sealed file types:

1. Create a folder called IRM_Sealed_File_Icons in the <*install_dir*>/weblayout/images directory.
2. Copy the icons with a dimension of 16x16 from the <IRM Component Directory>/Documentation/Installation of sealed file icons/Sealed File Icons/Gif/ directory.
3. Log in to Oracle Content Server and select **Admin Applets**.
4. Select the **Web Layout Editor** , select **Options**, then select **Query Results Pages**.
5. Choose the desired results page and click **Edit**.
6. Edit the text in the Text 2 section, adding code in the location where the icon is to be shown. Note that icons are available from the same directory for 32 and 64-bit icons.

   Sample code for using sealed icons is located in "Example Code for Icons for Sealed File Types Used in a Search Template" on page A-3.
7. Use the <$iconPath$> string in the location where the icon is to be displayed. For example, Download: sxlsx_16.gif: <$(VaultFileSize+1023)/1024$>K.

   This creates a download button with the correct sealed file icon and the file size.

5

Automatically Sealing Content Checked into Oracle Content Server

You may want users have sealing be transparent to them, or you may want users to be fully aware that they are sealing content.

You can ensure that content checked into Oracle Content Server is automatically sealed. You can accomplish this in many ways. You may choose to do this by user (through security groups), by location (through folders), or by other metadata fields through rules and profiles. You may want to permit users to unseal content upon future revisions, or you may want to prohibit unsealing of future revisions.

The following examples are typical of the types of mapping necessary to seal content via parameters defined in Folders, Security Groups, and Profiles:

5.1 Setting Default Metadata on a Folder for Sealing

An Oracle Content Server Administrator can define system default metadata on a folder. The general use case is for users to check in content directly to the folder and not through a check-in page. Be advised that this default metadata applies only to the initial check-in of the content. A user can change the metadata upon update or revision (if the user uses a check-in page), unless the profile that they use hides this metadata field. In addition, users can create subfolders, which will not have the same metadata set as the parent folder. For more information, see the *Folders and WebDAV Administration Guide*.

Use the following procedure to define system default metadata on a folder:

1. Make sure you are logged into Oracle Content Server as an administrator.
2. Open the **Administration** tray.
3. Create a Folder.
4. Expand the Folder Configuration link.

5. Click the **System Default Information Field Configuration link**. The System Default Information Field Configuration Page is displayed.
6. Specify the relevant sealer values to be applied to content upon check-in. For example, set the IRMProtection field to *Finance_Confidential*.
7. Click **Update**.

5.2 Creating a Security Group Specific to Sealing

An Oracle Content Server administrator can define a security group from within User Admin. This security group can then be used as the trigger for sealing of content checked into it. For more information, see the *Managing Security and User Access Guide*, which contains security information, and the *Managing Repository Content Guide*, which contains detailed examples for using rules and profiles.

Use the following procedure to define Oracle IRM-related security groups:

1. From within User Admin, click **Security**, then click **Permissions by Group**.
2. Click the **Add Group** button, and specify the group name *FinanceConfidential*. Assign roles to this group.*FinanceConfidential*.
3. Click **Close**.

5.3 Creating Rules and Profiles to Seal to One Context upon Check-in for all Defined Security Groups

An Oracle Content Server administrator can define rules and profiles from within Configuration Manager that automatically set sealing-related metadata fields and optionally hide these fields. For more information, see the *Managing Repository Content Guide*.

The following steps will create a profile called Finance_Confidential whose rule sets a derived value of Finance_Confidential into the IRMProtection field when a content item is checked in to one of these security groups: Public, Secure, or FinanceConfidential, all behind the scenes, without user awareness:

1. From within Configuration Manager, open the Rules tab, and select **Add**.
2. On the General tab, enter the name of the global rule in the Name field (for example, IRMProfileScenarioRule).
3. Optionally, enter a description for the rule, and ensure all check boxes are cleared.
4. Optionally, enter a description for the rule.
5. Add and define the IRMProtection field as follows.
    1. On the Fields tab, click **Add**.
    2. Select IRMProtection field from the Field Name drop-down option list.
    3. Click **OK**. The Add Rule Field screen is displayed.
    4. Select the **Hidden** display type from the Type drop-down option list.
    5. Check the **Is derived field** check box.
    6. Click the **Edit** button. The Script Properties screen is displayed.
    7. Click the **Add** button. Specify the name of the conditions to add. (For example 1, 2, and 3.)

8. For Condition 1, set **Field** to Security Group, **Operator** to Matches, and **Value** to FinanceConfidential. Set the **Value** field (below the clause) to Finance - Confidential. This value must match an Oracle IRM context.
9. For Condition 2, set **Field** to Security Group, **Operator** to Matches, and **Value** to Public. Set the **Value** field (below the clause) to Finance - Confidential. This value must match an Oracle IRM context.
10. For Condition 3, set **Field** to Security Group, **Operator** to Matches, and **Value** to Secure. Set the **Value** field (below the clause) to Finance - Confidential. This value must match an Oracle IRM context.
11. On the Custom tab, click the **Custom** check box to verify the following code is displayed:

```
<$if #active.dSecurityGroup like "FinanceConfidential"$>
    <$dprDerivedValue="Finance - Confidential"$> <$elseif
#active.dSecurityGroup like "Public"$>
    <$dprDerivedValue="Finance - Confidential"$> <$elseif
#active.dSecurityGroup like "Secure"$>
   <$dprDerivedValue="Finance - Confidential"$> <$endif$>
```

12. Click **OK** three times.

6. From within Configuration Manager, open the Profiles tab, and click **Select**.
7. Select Type from the Field Name drop-down option list.
8. Click **OK**
9. Click **Add** on the Profiles tab.
10. Enter the name of the profile, for example: Finance_Confidential.
11. Click **OK**.
12. Enter the profile description in the Description field.
13. Enter a label for the profile that clearly defines its use.
14. Select the value, that when entered by the user at check in, will trigger this rule. For example, **IRMProtection**.
15. Click Add to include the rules in this profile.
16. Select the RMProfileScenarioRule rule from the Name drop-down list.
17. Select a general priority placement from the Rule Priority drop-down option list (for example, top).
18. Click **OK**.

5.4 Creating Rules and Profiles to Seal to Separate Contexts Based on Security Group

This example is much like the previous example, except rather than sealing to one context for many security groups, this example seals to distinct contexts by specific security group. For example, when you add conditions, perform these steps:

1. For Condition 1, set **Field** to Security Group, **Operator** to Matches, and **Value** to FinanceConfidential. Set the **Value** field (below the clause) to Finance - Confidential. This value must match an Oracle IRM context.
2. For Condition 2, set **Field** to Security Group, **Operator** to Matches, and **Value** to Public. Set the **Value** field (below the clause) to Public. This value must match an Oracle IRM context.
3. For Condition 3, set **Field** to Security Group, **Operator** to Matches, and **Value** to Secure. Set the **Value** field (below the clause) to Secure. This value must match an Oracle IRM context.

These steps result in code that looks like this:

```
<$if #active.dSecurityGroup like "FinanceConfidential"$>
  <$dprDerivedValue="Finance - Confidential"$> <$elseif #active.dSecurityGroup
like "Public"$>
   <$dprDerivedValue="Public"$> <$elseif #active.dSecurityGroup like "Secure"$>
   <$dprDerivedValue="Secure"$> <$endif$>
```

5.5 Creating Rules and Profiles to Seal to Separate Contexts Based on Security Group and Account

This example is like the previous examples, except that this scenario requires a global rule and priority. A global rule is always evaluated and automatically affects the metadata fields even if it is not included in a profile or even if no profiles have been created. Global rules are evaluated first and can be superseded by specific profile rules. In addition, global rules have priority numbers, which determine the order in which the rule is evaluated, with lower priority rules being evaluated earlier. For more information on global rules see the *Managing Repository Content Guide*, which contains detailed examples for using rules and profiles.

To set a global rule, follow the steps to add a rule in previous examples, except rather than clearing check boxes, check the **Is global rule with priority** check box and optionally check the **Use rule activation condition**.

Then, when you add conditions, perform these steps:

1. For Condition 1, set **Field** to Security Group, **Operator** to Matches, and **Value** to FinanceConfidential. Then set **Field** to Account, **Operator** to Matches, and **Value** to Europe. Set the **Value** field (below the clause) to Finance_Europe. This value must match an Oracle IRM context.
2. For Condition 2, set **Field** to Security Group, **Operator** to Matches, and **Value** to FinanceConfidential. Then set **Field** to Account, **Operator** to Matches, and **Value** to Africa. Set the **Value** field (below the clause) to Finance_Africa. This value must match an Oracle IRM context.

These steps result in code that looks like this:

```
<$if #active.dSecurityGroup like "Finance" and #active.dAccount like "Europe"$>
    <$dprDerivedValue="Finance_Europe"$>
<$elseif #active.dSecurityGroup like "Finance" and #active.dAccount like
"Africa"$>$>
    <$dprDerivedValue="Finance_Africa"$>
<$endif$>
```

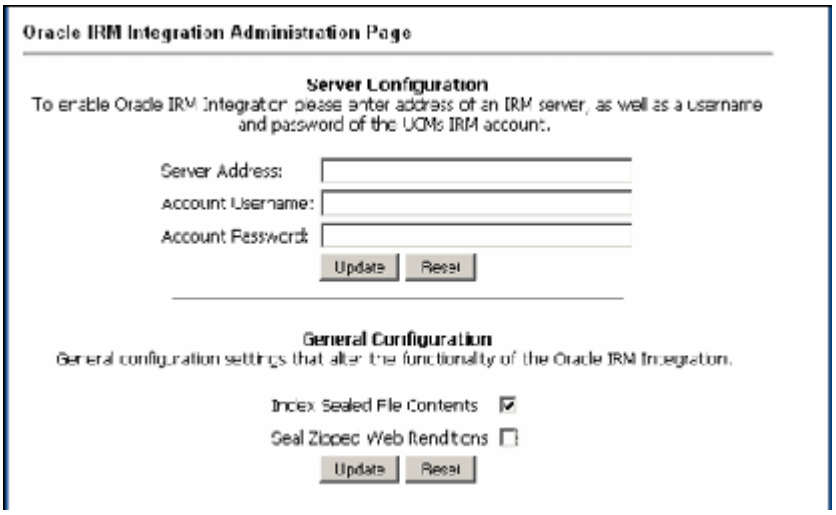
A

User Interface and Reference Information

This section covers the following topics:

- Oracle IRM Integration Administration Page
- IIS File Extensions for UCM-IRM Integration
- Example Code for Icons for Sealed File Types Used in a Search Template
- Uncommon Error Messages and Likely Causes

A.1 Oracle IRM Integration Administration Page



Administration Page Settings	Description
Server Address	Address of the license server (Oracle IRM Server).
Account Username	Account name for the Oracle Content Server account, as defined in Oracle IRM Server.
Account Password	Account password for the Content Server account, as defined in Oracle IRM Server.
Index Sealed File Contents	When selected, sealed file content will be indexed.
Seal Zipped Web Renditions	When selected, zipped web renditions will be sealed.

A.2 IIS File Extensions for UCM-IRM Integration

The following table shows the file extension types.

Ext.	Description	Sealed Mime Type	Unsealed Mime Type
stml	Sealed HTML	application/vnd.sealedmedia.softseal.html; application/vnd.sealed.html on MacOS	text/html
spdf	Sealed PDF	application/vnd.sealedmedia.softseal.pdf; application/vnd.sealed.pdf on MacOS	application/pdf
smov	Sealed QuickTime video	video/vnd.sealedmedia.softseal.mov; video/vnd.sealed.mov on MacOS	video/quicktime
sgif	Sealed Image	image/vnd.sealedmedia.softseal.gif; image/vnd.sealed.gif on MacOS	image/gif
spng	Sealed Image	image/vnd.sealed.png	image/png
sjpg	Sealed Image	image/vnd.sealedmedia.softseal.jpeg; image/vnd.sealed.jpeg on MacOS	image/jpeg
sdoc	Sealed Word	application/vnd.sealed.doc	application/msword
sxls	Sealed Ecel	application/vnd.sealed.xls	application/vnd.ms-excel
sppt	Sealed Power Point	application/vnd.sealed.ppt	application/vnd.ms-powerpoint
seml	Sealed Email	application/vnd.sealed.eml	application/msword
sxml	Seald XML	application/vnd.sealed.xml	text/xml; application/xml
sdot	Sealed Word Template	application/vnd.sealed.template	application/msword
sxlt	Sealed Excel Template	application/vnd.sealed.template	application/vnd.ms-excel
spot	Sealed Power Point Template	application/vnd.sealed.template	application/vnd.ms-powerpoint
srtf	Sealed Rich Text	application/vnd.sealed.rtf	text/richtext; text/enriched; application/rtf
stxt	Sealed Text	application/vnd.sealed.txt	text/plain
seml	Sealed Email (Word)	application/vnd.sealed.eml.doc	application/msword
seml	Sealed Email (Plain Text)	application/vnd.sealed.eml.txt	text/plain
seml	Sealed Email (RTF)	application/vnd.sealed.eml.rtf	text/richtext; text/enriched; application/rtf
scsf	Sealed CAD	application/vnd.sealed.csf	application/x-bravadtx
stif	Sealed Tiff	image/vnd.sealed.tiff	image/tiff
sdocx	Sealed Word Document	application/vnd.sealed.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document

Ext.	Description	Sealed Mime Type	Unsealed Mime Type
sdocm	Sealed Macro Enabled Word Document	application/vnd.sealed.docm	
sdotx	Sealed Word Template	application/vnd.sealed.dotx	
sdotm	Sealed Macro Enabled Word Template	application/vnd.sealed.dotm	application/vnd.ms-word.document.macroEnabled.12
sxlsx	Sealed Excel Workbook	application/vnd.sealed.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
sxlsm	Sealed Macro Enabled Excel Workbook	application/vnd.sealed.xlsm	application/vnd.ms-excel.sheet.macroEnabled.12
sxltx	Sealed Excel Template	application/vnd.sealed.xltx	application/vnd.openxmlformats-officedocument.spreadsheetml.template
sxltm	Sealed Macro Enabled Excel Template	application/vnd.sealed.xltm	application/vnd.ms-excel.template.macroEnabled.12
spptx	Sealed PowerPoint Presentation	application/vnd.sealed.pptx	application/vnd.openxmlformats-officedocument.presentationml.presentation
spptm	Sealed Macro Enabled PowerPoint Presentation	application/vnd.sealed.pptm	application/vnd.ms-powerpoint.presentation.macroEnabled.12
spotx	Sealed PowerPoint Template	application/vnd.sealed.potx	application/vnd.openxmlformats-officedocument.presentationml.template
spotm	Sealed Macro Enabled PowerPoint Template	application/vnd.sealed.potm	application/vnd.ms-powerpoint.template.macroEnabled.12

A.3 Example Code for Icons for Sealed File Types Used in a Search Template

The following code is representative of that which would be used to expose icons for sealed file types for Oracle Content Server customization for the interface and check-in screens.

Edit the text in the Text 2 section, adding the code in the location where the icon is to be shown. Note that icons are available from the same directory for 32 and 64-bit icons.

```
<table valign=bottom align=left width="100%" border=0><tr><td width="60%">

<$if dExtension like "doc"$>
    <$iconPath=HttpRelativeWebRoot&"images/format_icons/word.gif"$>
<$elseif dExtension like "xls"$>
```

```
    <$iconPath=HttpRelativeWebRoot&"images/format_icons/excel.gif"$>

<!-- Start of support for Oracle IRM sealed file icons -->

<$elseif dExtension like "sdoc"$>
    <$iconPath=HttpRelativeWebRoot&"images/IRM_Sealed_File_Icons/sdoc_16.gif"$>
<$elseif dExtension like "sxls"$>
    <$iconPath=HttpRelativeWebRoot&"images/IRM_Sealed_File_Icons/sxls_16.gif"$>

<!-- End of support for Oracle IRM sealed file icons -->


<$else$>
    <$iconPath=HttpRelativeWebRoot&"images/format_icons/icon-text.gif"$>
<$endif$>

Download: <a href="<$HttpCgiPath$>?IdcService=GET_FILE&dID=<$dID$>"><img
src="<$iconPath$>" border=0></a>

</td></tr></table>
```

A.4 Uncommon Error Messages and Likely Causes

The error messages in this section may have a cause that is not immediately obvious.

A.4.1 Oracle IRM: An error occurred while attempting to alter the database. Unable to execute query 'IRMUfileStorage(UPDATE FileStorage SET dFileSize = 40317 WHERE (dID = 604 AND dRenditionId ='primaryFile'))'. ORA-00942: table or view does not exist

This message is likely to have arisen because the File Store Provider component of Oracle Universal Content Management has not been installed, enabled and set up. This is a pre-installation task. The File Store Provider component of Oracle Universal Content Management must be installed before using the integration. The File Store Provider Installation and Administration Guide is available from the Oracle Technology Network.

A.4.2 Oracle IRM: Document check in could not continue because the UCM system has insufficient IRM rights to perform this action. Please make sure that UCM's IRM account has been assigned the correct rights on the IRM Server.

This message indicates either that the required Oracle IRM roles have not been created, or that the roles have not been located correctly, or that the roles have not been named exactly as given in the instructions in this document. See "Assigning Roles to the Context Template" on page 2-3. Note especially that the two administrator roles and one standard role must all be given the exact name "UCM-IRM integration" (without the quotes). If any other name is used for any of the roles, integration will fail.