Oracle® Fusion Middleware

User's Guide for Oracle IRM Desktop

11*g* Release 1 (11.1.1)

E12278-03

January 2011

ORACLE®

Oracle Fusion Middleware User's Guide for Oracle IRM Desktop, 11*g* Release 1 (11.1.1)

E12278-03

Copyright © 2007, 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Martin Wykes

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 software or related documentation 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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents x
Conventions x

1 About Oracle IRM and Sealed Content

1.1 About Oracle IRM 1-1
1.2 About Sealed Documents 1-2
1.3 About Rights 1-2
1.4 About Contexts 1-5
1.5 About Connecting to Oracle IRM Server 1-6
1.6 About Synchronizing with Oracle IRM Server 1-6
1.7 About Sealed Document Item Codes 1-6
1.8 About Sealed Email 1-7
1.9 About Microsoft Office Templates 1-7
1.10 About Sealed Multimedia Files 1-7
1.11 About Oracle IRM Fields and Watermarks in Sealed Documents 1-8

2 Installing Oracle IRM Desktop on Client Computers

2.1 System Requirements 2-1
2.2 Installing Oracle IRM Desktop 2-1
2.3 Upgrading Oracle IRM Desktop 2-2
2.4 Uninstalling Oracle IRM Desktop 2-2
2.5 Silent and Unattended Installations 2-3
2.5.1 About Silent and Unattended Installations 2-3
2.5.2 Oracle IRM Desktop Settings 2-4
2.5.3 Desktop Sealing Settings 2-4
2.5.4 Synchronization Manager Settings 2-5
2.5.5 Search Settings 2-6
2.5.6 Email Settings 2-7
2.5.7 Authentication Settings 2-8
2.5.8 Legacy Setting 2-8
2.5.9 Local Data Clean-Up Setting 2-8
2.5.10 Oracle IRM Background Process Startup Setting 2-9

2.5.11 Extracting the MSI File from the Self-Extracting Executable 2-9
2.6 Registry Key Policy Setting 2-10
2.7 Integrating Lotus Notes with Oracle IRM Desktop 2-10
2.7.1 Introduction to Lotus Notes Integration 2-10
2.7.2 Defining the Seal and Send Action 2-11
2.7.3 Propagating the Mail Template Change to All Mail Databases 2-11
2.7.4 Checking that the Lotus Notes Integration Works 2-12
2.8 Installing Oracle IRM Desktop in a Citrix Environment 2-12

3 Getting Started with Oracle IRM Desktop

3.1 Opening Sealed Documents 3-1
3.2 Sealing an Existing Document 3-2
3.3 Creating a New Blank Sealed Microsoft Office Document 3-3
3.4 Enabling Microsoft Office Integration 3-4

4 Working with Sealed Documents

4.1 Opening Sealed Documents 4-1
4.1.1 About Opening Sealed Documents 4-1
4.1.2 Opening a Sealed Document in a File Browser 4-1
4.1.3 Opening a Sealed Document in a Microsoft Office Application 4-2
4.2 Editing Sealed Documents 4-3
4.2.1 About Editing Sealed Documents 4-3
4.2.2 About Using the Clipboard while Editing Sealed Documents 4-3
4.3 Creating New Sealed Documents 4-4
4.3.1 About Creating New Sealed Documents 4-4
4.3.2 Using Windows Explorer to Create a New Microsoft Office Document that is Sealed from the Outset 4-4
4.3.3 Using Microsoft Office to Create a New Document that is Sealed from the Outset .. 4-5
4.3.4 Creating a Sealed Version of an Existing Unsealed Document 4-6
4.4 Saving Changes to Sealed Documents 4-6
4.4.1 About Saving Changes to Sealed Documents 4-6
4.4.2 Saving Changes to A Sealed Document 4-7
4.5 Changing the Contexts That Documents are Sealed to 4-7
4.5.1 About Changing Contexts 4-7
4.5.2 Changing the Context That a Document is Sealed To 4-7
4.6 Unsealing Sealed Documents 4-8
4.6.1 About Unsealing Sealed Documents 4-8
4.6.2 Unsealing a Sealed Document 4-8
4.7 Searching Sealed Documents 4-8
4.7.1 About Searching Sealed Documents 4-8
4.7.2 Enabling Sealed Documents to Be Searched 4-9
4.7.3 Configuring for the Microsoft Indexing Service 4-10
4.7.4 Configuring Search Logging 4-10
4.8 Printing Sealed Documents 4-10
4.8.1 About Printing Sealed Documents 4-11
4.8.2 Printing a Sealed Document 4-11
4.9 Screen Capturing Sealed Documents 4-11

4.9.1 About Screen Capturing Sealed Documents 4-11
4.9.2 Sharing a Sealed Presentation During a Web Conference 4-11
4.9.3 Capturing the Image of a Sealed Document 4-12
4.10 Using Sealed Microsoft Excel Spreadsheets 4-12
4.10.1 About Sealed Microsoft Excel Spreadsheets 4-12
4.10.2 Linking Sealed Microsoft Excel Spreadsheets 4-13
4.10.3 Updating Links Between Previously Unsealed Spreadsheets 4-13
4.11 Using Sealed Microsoft Office Templates 4-14
4.11.1 About Using Sealed Microsoft Office Templates 4-14
4.11.2 Creating a Sealed Microsoft Office Template from Within Microsoft Office 4-14
4.11.3 Creating a Sealed Microsoft Office Template Using Windows Explorer 4-15
4.11.4 Editing Sealed Microsoft Office Templates 4-15

5 Using Sealed Email

5.1 Creating and Sending Sealed Email 5-1
5.1.1 About Creating and Sending Sealed Email 5-1
5.1.2 Creating and Sending Sealed Email using an Integrated Email Application 5-2
5.1.3 Creating and Sending Sealed Email using an Existing Document Attachment 5-2
5.1.4 Creating and Sending Sealed Email using Sealed Email Document Format 5-2
5.2 Opening Sealed Email Messages and Sealed Attachments 5-3
5.3 Creating Sealed Email Replies 5-4
5.3.1 Creating a Sealed Reply to an Unsealed Message 5-4
5.3.2 Replying to a Sealed Email 5-5
5.4 Forwarding Sealed Email 5-5
5.4.1 Forwarding Sealed Email Without Amendment 5-5
5.4.2 Forwarding Sealed Email With Amendments 5-6
5.4.3 Sealing and Forwarding an Email that was Received Unsealed 5-6

6 Working With Oracle IRM Fields and Watermarks

6.1 About Oracle IRM Fields and Watermarks 6-1
6.2 Adding Oracle IRM Fields in Microsoft Word 6-1
6.2.1 Adding an Oracle IRM Field to a Microsoft Word Document 6-1
6.2.2 Registering Oracle IRM Fields as Microsoft Word Document Properties 6-2
6.2.3 Using Oracle IRM Fields That Have Been Registered As Microsoft Word Document Properties 6-3
6.3 Adding Oracle IRM Fields in Microsoft Excel 6-3

7 Managing Oracle IRM Rights

7.1 About Obtaining and Managing Your Rights 7-1
7.2 Managing Rights on a Shared Computer 7-2
7.3 Connecting to Oracle IRM Server Manually 7-2
7.4 Synchronizing Your Rights Manually 7-3
7.5 Checking In Your Rights Manually 7-3
7.6 Clearing Your Password 7-4

8 Using Oracle IRM Desktop with Microsoft SharePoint

8.1 Using Sealed Documents With Microsoft SharePoint 8-1
8.2 Modifying a Microsoft SharePoint Server for Use with Oracle IRM 8-2
8.3 Enabling Search With Microsoft Sharepoint 2007 8-4

9 Oracle IRM Desktop Reference

9.1 List of Oracle IRM Fields 9-1
9.2 Frequently Asked Questions 9-2
9.3 Troubleshooting 9-5
9.3.1 Proxy Issues 9-5
9.3.2 Sealed Documents Block Screen Captures 9-6
9.4 Formats 9-6
9.5 Registry Key Information 9-9

A User Interface

A.1 Oracle IRM Desktop Options Dialog A-1
A.1.1 General Tab A-1
A.1.2 Desktop Sealing Tab A-2
A.1.3 Servers Tab A-4
A.1.4 Update Rights Tab A-5
A.1.5 Search Tab A-6
A.1.6 Email Tab A-7
A.1.7 About Tab A-8
A.1.8 Add Server Dialog A-9
A.1.9 Search Log Configuration Dialog A-10
A.1.10 Synchronization Log Configuration Dialog A-10
A.1.11 Indexing Service Configuration Dialog A-11
A.2 Sealed Email Options Dialog A-12
A.2.1 Signature Tab A-13
A.2.2 Email Template Tab A-13
A.2.3 Email Body Tab A-14
A.2.4 Sealed Reply Settings Tab A-15
A.2.5 Sealed Email Format Tab A-15
A.3 Oracle IRM Desktop Control Panel Dialog A-16
A.3.1 Properties Tab A-16
A.3.2 Rights Tab A-17
A.3.3 Account Tab A-18
A.4 General Features A-19
A.4.1 Oracle IRM Privacy Policy Dialog A-20
A.4.2 Select Context Dialog A-20
A.4.3 Change Item Code Dialog A-21
A.4.4 Status Page Dialog A-22
A.4.5 File Report Dialog A-23
A.4.6 Sealed File Properties (Oracle IRM) Tab A-24
A.4.7 Oracle IRM Server Connection Test Dialog A-25
A.4.8 Oracle IRM Desktop Support Information Dialog A-25

A.4.9 Change Password Dialog (10*g* only) A-26
A.4.10 Protected View Message Dialog A-27
A.5 Oracle IRM Desktop Toolbars A-27
A.5.1 Oracle IRM Desktop Toolbar in Internet Explorer A-27
A.5.2 Oracle IRM Desktop Toolbar in Microsoft Office A-28
A.5.3 Oracle IRM Desktop Toolbar in Microsoft Office 2007 and Microsoft Office 2010. A-28

Index

Preface

Oracle Information Rights Management (Oracle IRM) is an information security solution that uses encryption to 'seal' content (documents and emails). Access to the decryption keys is carefully controlled, so that only authorized end users can open and use the sealed content, regardless of where it is stored and used.

Oracle IRM Desktop is a small application that must be installed on every computer that will be used to seal documents using the Oracle IRM encryption technology. Oracle IRM Desktop must also be installed to read documents that have been sealed using this technology. Oracle IRM Desktop is the client software for Oracle IRM Server, which is installed and maintained centrally by organizations wanting to produce sealed documents. The Oracle IRM Desktop client must have access to the Oracle IRM Server installation so that the rights of users to read sealed documents can be ascertained. Access to Oracle IRM Server must be regular, but need not be continuous: Oracle IRM Desktop caches user rights locally and will allow access to sealed documents for a pre-determined period, usually a few days, before access to Oracle IRM Server is required.

This user guide contains procedures for using the Oracle IRM Desktop client product and conceptual information explaining why and when to use these procedures. This guide also contains descriptions of the user interface for the product.

Audience

This document is intended for end users of Oracle IRM Desktop.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an

otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

For more information, see the following documentation.

- *Oracle Fusion Middleware Developer's Guide for Oracle IRM Server*
- *Oracle Fusion Middleware External Users Support Guide for Oracle IRM Desktop*
- *Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server* (This guide is also available as the online help for the Oracle IRM Server product.)

Conventions

The following 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 specific values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
back slashes (\)	Back slashes are used to separate the directory levels in a path name. A back slash will always appear after the end of a directory name.

1

About Oracle IRM and Sealed Content

This section covers the following topics:

- About Oracle IRM
- About Sealed Documents
- About Rights
- About Contexts
- About Connecting to Oracle IRM Server
- About Synchronizing with Oracle IRM Server
- About Sealed Document Item Codes
- About Sealed Email
- About Microsoft Office Templates
- About Sealed Multimedia Files
- About Oracle IRM Fields and Watermarks in Sealed Documents

1.1 About Oracle IRM

Oracle Information Rights Management (Oracle IRM) is an information security solution that uses encryption to 'seal' content (documents and emails). Access to the decryption keys is carefully controlled, so that only authorized end users can open and use the sealed content, regardless of where it is stored and used.

Oracle IRM enables authorized users to create and use sealed content transparently within existing desktop applications, such as Microsoft Office, Adobe Reader and Lotus Notes, without requiring detailed knowledge of keys or passwords. A one-time installation of the Oracle IRM client software, Oracle IRM Desktop, supports current and previous versions of these standard desktop applications, and continues to protect and track sealed documents and emails while they are in use within them. See Section 9.4, "Formats".

Oracle IRM also continues to protect and track sealed content when it is stored and used on desktops beyond the firewall of the originating organization. Recipients of sealed documents and emails may be authorized by the originating organization to use them in one or more different ways, including reading them, replying to them, editing them, searching them, copying them, and printing them.

When the originator of a sealed document or email decides that the content is no longer valid, or when the originator decides to change who can use a sealed document

or email, the rights can be revoked and the recipient may find that they can no longer read it.

1.2 About Sealed Documents

Sealed documents are encrypted files that are accessible only to authorized users. They have distinctive icons and file extensions. See Section 9.4, "Formats" for a full list.

The Oracle IRM solution supports a wide range of document formats, including Microsoft Word, Excel, and PowerPoint, PDF, HTML, RTF and text, and various image and movie formats.

Supporting popular document formats enables the Oracle IRM solution to fit seamlessly into existing working practices, ensuring the security and confidentiality of critical business information.

Your ability to work with a specific sealed document depends on the rights defined for you in the contexts to which the document is sealed. For example, your rights to work with documents in a Top Secret context and a Confidential context might be very different.

1.3 About Rights

Rights control what you can and cannot do with sealed documents. Your rights to a specific sealed document can range from none (so you cannot even open the document), to Open (so you can read it on your computer screen, but do nothing else with it), through a range of rights to, for example, edit, print, and search the document. Your rights also control your ability to create new sealed documents.

Your rights can be changed over time, can differ from the rights of other users, and can differ from one sealed document to another. Your rights to a specific document depend on what context that document is sealed to. For example, your rights to documents in a Top Secret context might be much more restricted than for documents in a Confidential context.

Some rights effectively include others (for example, if you have the Edit right, you also get the Annotate and Interact rights), and some rights require others (for example, if you have the Edit right, you need the Open right to access the document, and you need the Reseal right so that you can save your edits).

When you are viewing a specific sealed document, you can see your rights for that document on the Rights tab of the Oracle IRM Desktop Control Panel. The Rights tab lists only rights that are relevant to the type of sealed document you are viewing.

This guide tells you the rights you need to perform common Oracle IRM tasks. If you need to perform tasks for which you do not have rights, you should ask an Oracle IRM Server administrator whether you can be given the necessary rights.

Note to Oracle IRM Server administrators: The "rights" available in Oracle IRM Desktop are created by assigning "features", and setting constraints, within Oracle IRM Server. See the *Administrator's Guide for Oracle IRM Server* for full details.

The complete set of rights is described in Table 1–1.

Table 1–1 Rights

Right	Description	Usage notes
Accessibility	Relaxes protection of sealed files so the use of accessibility tools and features is not blocked for sealed files. It does this by turning off program protection, screen capture protection, and keyboard protection in the file.	Some accessibility tools might work even without this right.
Annotate	Allows you to add comments in Microsoft Excel and Microsoft Word documents (DOC and RTF formats).	The ability to add comments may be the only editing you can do on sealed documents. In Microsoft Word, the Annotate right negates the Interact right.
Copy	Allows you to copy content from a sealed document and paste it into any other document. Allows you to change the context of a sealed document to any other context that you have access to.	Applicable only to Microsoft Office, email, and PDF. If you have the Copy right, you do not have, or need, the Copy To right. This is because Copy To is more restrictive that Copy. Use of copy and paste within a specific sealed document does not require any rights other than the Edit right.
Copy To	Allows you to copy content between documents that are sealed to the same context. Allows you to copy content from a sealed document and paste it into a document that is sealed to another context, but only if this is a trusted context. Allows you to change the context of a sealed document to another context that is a trusted context. Allows you to make a copy of a sealed document and then change the context of the copy to another context that is a trusted context. **Important:** Copy To is not directly selectable as a right. Instead, it is assigned by setting Exporting Content to "Allow with restrictions" on the Constraints tab of a role.	Trusted contexts are set up in Oracle IRM Server. You can check which contexts have been set up as trusted contexts for the current sealed document (there will be at least one), by looking under "Trusted Destinations" on the Rights tab of the Oracle IRM Desktop Control Panel. If you have rights to copy content to other contexts, you also need the relevant rights in those contexts. For example, to copy content to a document in another context, you need the right to open and edit documents in that context. To change the context of a sealed document, right-click it in a file browser and select **Reseal To**. You need the Copy To right for the current context and the Seal right for the destination context. Use of copy and paste within a specific sealed document does not require any rights other than the Edit right. Even with the Copy To right, you may sometimes not be able to copy content between documents (for example, in some multi-process environments).
Edit	Allows you to edit Microsoft Office documents.	The Edit right includes the Edit Tracked, Annotate, Interact, and Formulae rights.

Table 1–1 (Cont.) Rights

Right	Description	Usage notes
Edit Tracked	Allows you to edit Microsoft Office documents, but enforces the use of the track changes feature of Microsoft Word.	The Edit Tracked right is included in the Edit right.
Formulae	Allows you to select and view formulae (formulas) in Microsoft Excel workbooks.	The Formulae right is included in the Edit and Edit Tracked rights.
Interact	Allows you to enter data into Form fields in Microsoft Word documents. Allows you to enter data into unprotected cells of Microsoft Excel documents.	The Interact right is included in the Edit and Edit Tracked rights. In Microsoft Word, the Interact right is ineffective if the Annotate right has also been granted.
Open	Allows you to open a sealed document and view it on screen.	The Open right might be the only right you have to a document. The Open right is a prerequisite for all other rights except Seal and Search.
Print	Allows you to print documents to create paper copies.	The Print right is included in the Print to File right.
Print To File	Allows you save a document as a print file, or send documents to a virtual printer (for example, Adobe PDF).	Print To File includes the Print right.
Program	Allows you to use macros within a sealed document to manipulate the document's content.	
Reply	Allows you to edit a sealed email to create a reply.	You also need Reseal to save your email edits. You do not need Edit when replying to sealed email. Reply does not allow you to create new sealed emails. That requires the Seal right.
Reply Tracked	Allows you to edit a sealed email to create a reply, but enforces the track changes feature.	You also need the Reseal right to save your email edits. Reply Tracked does not allow you to create new sealed emails. That involves creating a new sealed document, and therefore requires the Seal right.
Reseal	Allows you to save edits to a sealed document or to a sealed email reply.	When you save a sealed document, you can use a different filename, but the new file is subject to exactly the same rights as its source document. The Reseal right is not associated with the **Reseal To** option available when right-clicking a sealed file in a file browser (such as Windows Explorer). For an explanation of the **Reseal To** option, see the Copy To right.

Table 1–1 (Cont.) Rights

Right	Description	Usage notes
Save Unsealed	Allows you to create an unsealed copy of a sealed document.	This right enables you to create an unprotected copy of a sealed document. An unsealed document can be created using the **Save As** option in applications. An unsealed document can also be created using the **Unseal** option when you right-click a sealed file in a file browser (such as Windows Explorer).
Screen Capture	Allows you to take screen captures of sealed documents. (See Section 4.9, "Screen Capturing Sealed Documents".)	Apart from its obvious use, you might be given this right if you have a legitimate reason to use an application that sends images from your computer to another computer, such as a web presentation product.
Seal	Allows you to create a new sealed document or email.	Typically, if you have the Seal right, you also have the Edit right, so that you can edit the documents you create. However, if you have been given the Seal right so that you can use sealed email, it is possible that you will not have the Edit right. Sealed email usage requires the Seal right for email creation, and the Reseal and Reply (or Reply Tracked) rights for replying.
Search	Allows you to use Microsoft Windows search facilities to search the content of sealed documents.	Unless you have this right, searches will not include the content of sealed documents. Searching sealed PDF requires a search filter from Adobe as well as the Search right.
Set Item Code	Allows you to manually set the item code of a sealed document.	Item codes are mostly allocated and updated automatically, and reflect the name of a sealed document and the time that it was sealed. Not all sealed documents have item codes. You might be given the right to allocate item codes manually. If so, you will see some extra options and messages when working with sealed documents, and you should be trained to understand what you need to do.

1.4 About Contexts

A context is a type or grouping of sealed content. For example, you might have contexts for secret sales matters, confidential sales matters, proprietary research matters, confidential partner communications, and so on.

The rights defined for each context can be very different so, for example, you might have rights to open, edit, and print confidential sales documents, but only the right to open secret sales documents, and no rights at all for research documents. Different users have different rights in different contexts.

If you are the owner or creator of sensitive documents, you can work with the rights administrator (or, in Oracle IRM terms, the "domain manager") to create one or more contexts to protect that information. For example, if you are developing a new product, you might create contexts to protect the requirements, specifications, designs, market projections, competitive information, legal information, patents, and so on. Your domain manager can help you decide whether you need new contexts, or whether existing contexts are suitable for your information.

1.5 About Connecting to Oracle IRM Server

Before you can create or read sealed documents, your installation of Oracle IRM Desktop must be connected to the server (Oracle IRM Server) that holds the user and context information for the documents to be created or read.

If you have been sent a sealed document and want to read it, simply opening the document will initiate connection to the server. You may be asked to provide login details, after which you will be able to use the sealed document to the extent that your rights allow. You will find that the server to which you have been connected is listed on the Servers tab of the Oracle IRM Desktop Options dialog.

If you wish to seal a document to a context hosted by a server that is not yet listed on the Servers tab, you will need to connect to that server manually. See Section 7.3, "Connecting to Oracle IRM Server Manually".

1.6 About Synchronizing with Oracle IRM Server

If you are permitted to work offline, your local cache of rights is updated by synchronizing to connected servers. This will allow you to keep working with sealed documents even when you are disconnected from the network and cannot contact the server. Typically, your cached rights allow you to keep using documents for several days before being required to contact the server.

Synchronization is almost completely automatic. Typically, it runs daily during standard office hours, but the schedule is controlled by the administrator of the server.

If synchronization fails for any reason, the application displays a failure message and automatically retries at intervals.

You can initiate synchronization manually at other times: for example, if someone notifies you that your rights have changed, and you want to synchronize immediately rather than wait for the automatic process. See Section 7.4, "Synchronizing Your Rights Manually".

1.7 About Sealed Document Item Codes

By default, all documents in a given context are subject to the same rights. However, the need may arise for exceptions to be made for specific documents. For example, it might be necessary to allow an auditor access to a specific secret merger document, but not to all secret merger documents.

To support such exceptions, every sealed document has an item code.

In most cases, item codes are allocated and managed automatically. In rare cases, users may be authorized to allocate and change item codes manually. This enables a user to, for example, create several different documents all with the same item code, enabling the documents to be handled as a unit for the allocation of rights.

Item codes are changed or retained depending on your rights. If you have the Seal right, then when you save (or save as) any edits to a document, a new item code will be created for that document. If you have the Reseal right, then every time you save the document, the same item code will be used.

1.8 About Sealed Email

In any business environment, confidential and sensitive information is entrusted to email communications. The Oracle IRM solution provides the tools you need to enable you to seal email just as you seal other types of content.

To work effectively with sealed email, you need to:

- Create and send sealed email.
- Open sealed email that you receive.
- Open sealed files that are sent as attachments to emails.
- Create and send sealed replies.
- Forward sealed emails.

Oracle IRM Desktop enables all of the above so that you can participate in sealed email threads. See Section 5, "Using Sealed Email".

Your rights to create and reply to sealed email are managed separately from your rights to create and edit other types of sealed document.

1.9 About Microsoft Office Templates

The Oracle IRM solution supports two ways of using templates to enable organizations to create sealed documents consistently:

- You can use sealed Microsoft Office templates to create Microsoft Word, Excel, and PowerPoint documents consistently.
- You can create sealed documents from regular Microsoft Office templates using the Oracle IRM menu within Microsoft Office.

See Section 4.11.1, "About Using Sealed Microsoft Office Templates".

In each case, your templates can contain Oracle IRM fields that help to remind users of the sensitive nature of the documents created from them. For example, a template might have headers and footers that contain fields that identify the context of the documents, and the name of the user who opens a specific copy.

1.10 About Sealed Multimedia Files

Oracle IRM supports a range of video file formats. You will generally need the Open right to view sealed video files. See Section 1.3, "About Rights".

You can seal video files in the same way as you seal other types of file. For example, users of the Oracle IRM Desktop can select video files in Windows Explorer and select **Seal To** from the **File** menu. You are prompted to select a context for the files.

When you open sealed video files, the Oracle IRM Desktop toolbar provides buttons for playing, pausing, and stopping the file.

You will need to have QuickTime Player installed on your PC to be able to play back sealed video files.

1.11 About Oracle IRM Fields and Watermarks in Sealed Documents

If you are an author of sealed documents, you can add Oracle IRM fields to your document sources before sealing. When someone opens a sealed document that contains Oracle IRM fields, the fields help to remind the reader that the document is sensitive. Oracle IRM fields used as watermarks can help to make a printed copy of the document traceable in the event that it falls into the wrong hands.

You can use Oracle IRM fields in Microsoft Word and Microsoft Excel. See Section 6, "Working With Oracle IRM Fields and Watermarks".

For these applications, you can also create templates that contain a set of Oracle IRM fields, and apply them consistently to new documents. For example, in Microsoft Word, you can create a sealed Word template that contains the fields in headers and footers, and use that template to create a new sealed document.

When viewing the unsealed source, the fields appear as field names or placeholder strings. However, when sealed and viewed with Oracle IRM Desktop available, the fields are transformed to contain the relevant data. For example, `irm-account-name` might be transformed to John.Smith, the name of the user who opens a specific copy of a sealed document.

2

Installing Oracle IRM Desktop on Client Computers

Oracle IRM Desktop can be installed by anyone intending to use the product to read documents that have been sealed using Oracle IRM encryption technology, or to seal documents. The person installing the product must have administrator rights for the computer on which it is being installed. Many organizations do not give administrator rights to individual users, in which case the organization's IT specialists should install the product.

This section explains the process of installing Oracle IRM Desktop on client computers. It covers these topics:

- System Requirements
- Installing Oracle IRM Desktop
- Uninstalling Oracle IRM Desktop
- Upgrading Oracle IRM Desktop
- Silent and Unattended Installations
- Integrating Lotus Notes with Oracle IRM Desktop
- Installing Oracle IRM Desktop in a Citrix Environment

2.1 System Requirements

Supported operating systems, browsers, and third-party applications

The latest requirements are detailed on the certification matrix documents available from the following location on the Oracle Technology Network:

`http://www.oracle.com/technology/software/products/ias/files/fusion_certification.htm`

Installation privileges

The installation requires administrator privileges or elevated privileges.

2.2 Installing Oracle IRM Desktop

Note: If you are reading this section in the online help, then Oracle IRM Desktop is already installed.

Oracle IRM Desktop is typically downloaded and installed from a web page. The web page might be hosted by Oracle IRM, or by another organization. Typically, you will be told the address of the download site.

1. Close all instances of Microsoft Word, PowerPoint, Excel, and Outlook.
2. Uninstall any previous version of Oracle IRM Desktop or the SealedMedia Unsealer or Desktop software.
3. Go to the Oracle IRM Desktop download site.
4. Follow any instructions on the Oracle IRM Desktop download site for downloading the installation file.
5. Run the downloaded installation file and follow the installation wizard.

Do not attempt to install Oracle IRM Desktop on a mapped drive or on a drive defined using the `subst` command.

Silent and unattended installations are also supported (see Section 2.5, "Silent and Unattended Installations").

2.3 Upgrading Oracle IRM Desktop

You can upgrade to this version of Oracle IRM Desktop from version 5.5 onwards, by running the installation wizard on the computer that has the older version.

For versions earlier than 5.5, or from any version of SealedMedia Unsealer or Desktop, you can upgrade to this version only by uninstalling the older version and installing this one.

Caution: When upgrading from versions of Oracle IRM Desktop earlier than version 11.1, you will lose the rights that are stored locally to use sealed documents (the rights that enable you to continue working when you are offline). When this happens, you will have to obtain new rights by going online and synchronizing with the server. For this reason, do not begin an upgrade unless you have online access to the server. (You can cause resynchronization by opening an existing sealed file.)

2.4 Uninstalling Oracle IRM Desktop

Caution: If you uninstall Oracle IRM Desktop from a computer, you will not be able to use the computer to read sealed documents.

To uninstall Oracle IRM Desktop from a computer, you need administrator rights for that computer.

Use the Control Panel Add/Remove Programs dialog to uninstall Oracle IRM Desktop, if required. Alternatively, run the installer and you will be offered the option to uninstall.

Uninstalling Oracle IRM Desktop does not delete your local rights database from your system. If you re-install, your existing rights will still be available.

2.5 Silent and Unattended Installations

Silent and unattended installations are intended to be made by IT specialists with full administrator rights for all the client computers.

This section contains the following topics:

- About Silent and Unattended Installations
- Oracle IRM Desktop Settings
- Desktop Sealing Settings
- Synchronization Manager Settings
- Search Settings
- Email Settings
- Authentication Settings
- Legacy Setting
- Local Data Clean-Up Setting
- Oracle IRM Background Process Startup Setting
- Extracting the MSI File from the Self-Extracting Executable

2.5.1 About Silent and Unattended Installations

The Oracle IRM Desktop installation package is a self-extracting executable that contains an MSI installer. If you are the network administrator for many Oracle IRM Desktop users, you can use the installer to manage silent installations and preconfigure settings.

You can either pass arguments to the self-extracting executable, or run it once to extract the MSI installer and then use `msiexec.exe` to pass arguments directly to it. However, if using GPO (Group Policy Object) then the standard way to set parameters is to use Orca from the Windows SDK to create MST files that set the required arguments, then to apply that transform and the MSI together in GPO.

The following example shows how to pass arguments directly to an extracted MSI installer:

```
msiexec /i "OracleIRMDesktop_en.msi" /qn EMAIL_OUTLOOK_ACTIVATED=1
```

The following shows how to achieve the same effect by passing arguments to the self-extracting executable:

```
"OracleIRMDesktop_en.exe" /v' /qn EMAIL_OUTLOOK_ACTIVATED=1'
```

The `/v` argument signifies the arguments enclosed by the single quotes are to be passed to the MSI installer within the executable.

Most of the configurable settings relate to the functional subcomponents of Oracle IRM Desktop:

- Oracle IRM Desktop - controls access to sealed documents
- Desktop sealing - integrates sealing options into Windows Explorer
- Synchronization manager - automates rights synchronization
- Search integration - integrates with search facilities

- Email integration - integrates with popular email applications such as Microsoft Outlook

After installation, the above settings are accessible by right-clicking the Oracle IRM icon in the Windows notification area (tooltray) and selecting Options.

There are also configurable settings for:

- authentication
- legacy server authentication types
- clean-up of local data

The following sections provide information about the configurable settings. All components have valid defaults that enable a user to open and work with sealed documents, subject to their rights, immediately after installation. Configuration of settings during installation is optional.

2.5.2 Oracle IRM Desktop Settings

The Oracle IRM Desktop settings that you can preconfigure are as follows:

Property and description	UI Option	Values	Default
UNSEALER_OFFICEENABLED Determines whether the integration with Microsoft Office is enabled.	Enable Microsoft Office support	0 = disabled 1 = enabled	1
UNSEALER_SHOWTRAYICON Determines whether the Oracle IRM notification icon is shown.	Display in system tray	0 = hide 1= show	1
UNSEALER_SHOWIRMBAR Determines whether the Oracle IRM information bar is displayed within Microsoft Office for sealed documents.	Display Sealed Office information bar	0 = hide 1 = show	1

These options relate to settings that appear on the Oracle IRM Desktop tab of the Oracle IRM Desktop Options dialog.

2.5.3 Desktop Sealing Settings

The Desktop sealing settings that you can preconfigure are as follows:

Property and description	UI option	Values	Default
DESKTOPSEALER_ACTIVATED Determines whether the sealing of content through Oracle IRM Desktop is enabled.	Enable Desktop Sealing	0 = disabled 1 = enabled	1
DESKTOPSEALER_ CLASSIFICATIONMRUSIZE Sets the maximum number of recently used contexts displayed in Seal To menus in Windows Explorer.	Recently Used Context List	integer	5

Property and description	UI option	Values	Default
DESKTOPSEALER_DELETESOURCEFILES Determines whether the original unsealed files are deleted after sealed versions of them are created, or whether the original unsealed files are moved to the recycle bin, and whether the user is prompted before these actions.	Delete original file(s) after sealing	0 = No deletion 1 = Original files moved to recycle bin, with confirmation 2 = Original files permanently deleted, with confirmation 3 = Original files moved to recycle bin, with no confirmation 4 = Original files permanently deleted, with no confirmation	0

These settings relate to options on the Desktop Sealing tab of the Oracle IRM Desktop Options dialog.

2.5.4 Synchronization Manager Settings

The synchronization manager settings that you can preconfigure are as follows.

Property and description	Values	Default
SYNCINITIALSERVERS Determines a set of servers to which Oracle IRM Desktop will be initially synchronized, as shown in the list of synchronized servers. The set of servers has to be encoded into a compound string in the form: <url1>|<value1>[,<url2>|<value2>,<url3>|<value3>,...]	For example, to add the following servers: ■ irm1.example.com ■ irm2.example.com ■ irm3.example.com the string to pass in the SYNCINITIALSERVERS property is: SYNCINITIALSERVERS="https://irm1.example.com/irm_desktop|1,https://irm2.example.com/irm_desktop|1,https://irm3.example.com/irm_desktop|0" where the value 1 means that synchronization for the server is enabled and the value 0 means that synchronization for the server is disabled.	None

Property and description	Values	Default
SYNCLOCKEDSERVERS Determines a set of servers that are locked from user modification. If a locked server appears in the list of synchronized servers, the user cannot disable synchronization for that server, nor remove it from the list of synchronized servers. The presence of a server in this set does not add it to the list of synchronized servers. Locked servers will appear in the list of synchronized servers only because they have been added through the SYNCINITIALSERVERS property or because a user has added it.	For example, to lock the following servers: ▪ irm1.example.com ▪ irm2.example.com the string to pass in the SYNCLOCKEDSERVERS property is: SYNCLOCKEDSERVERS ="https://irm1.example.com/irm_ desktop|1,https://irm2.example.com/irm_desktop|1" where the value 1 means the server is locked. A value of 0 would mean that the server is unlocked, but this has the same effect as simply not listing the server.	None

These settings relate to the server list on the Synchronization tab of the Oracle IRM Desktop Options dialog.

Property and description	UI option	Values	Default
SYNC_LOGLEVEL Determines the level of logging of synchronization messages to the Windows event log. The messages are categorized as low-level, standard, and detailed.	Synchronization Messages	0 = no messages 1 = success notifications 2 = error notifications only; no success notifications 3 = 7 =	2

These settings relate to the checkboxes on the Synchronization Log Configuration dialog.

2.5.5 Search Settings

The search settings that you can preconfigure are as follows:

Property and description	UI option	Values	Default
SEARCH_ENABLED Determines whether searching of sealed documents is enabled.	Enable Search	0 = disabled 1 = enabled	[1]
SEARCH_REPORTERRORS Determines whether search errors are reported in the Windows event log.	Search Error Messages	0 = do not report 1 = report	1
SEARCH_REPORTWARNINGS Determines whether search warnings are reported in the Windows event log.	Search Warning Messages	0 = do not report 1 = report	0

Property and description	UI option	Values	Default
SEARCH_REPORTINFORMATION Determines whether search information is reported in the Windows event log.	Search Information Messages	0 = do not report 1 = report	0

These settings relate to the option on the Search tab of the Oracle IRM Desktop Options dialog, and to the checkboxes on the Search Log Configuration dialog.

2.5.6 Email Settings

The email settings that you can preconfigure are as follows:

Property and description	UI option	Values	Default
EMAIL_OUTLOOK_ACTIVATED Determines whether the sealed email integration is activated within Microsoft Outlook.	Microsoft Outlook	0 = deactivated 1 = activated	0
EMAIL_LOTUSNOTES_ACTIVATED Determines whether the sealed email integration is activated within Lotus Notes.	Lotus Notes	0 = deactivated 1 = activated	0
EMAIL_USECUSTOMTEMPLATE Determines whether a Microsoft Word template file should be used when sending sealed emails.	Use Custom Template	0 = do not use custom template 1 = use custom template	0
EMAIL_CUSTOMTEMPLATEFILE Specifies the Microsoft Word template file to use when sending sealed emails. The file could contain watermarking that you want added to every sealed email you send.	Specify the Word template file....	path and filename	none
EMAIL_BODYFILE Specifies the RTF or HTML file that contains the unsealed body text of sealed emails.	Template Body File	path and filename	none
EMAIL_BODYTYPE Determines the type of the unsealed body text of sealed emails.	Unsealed Email Body	0 = blank 1 = plain text 2 = RTF or HTML file	1
EMAIL_BODYTEXT Specifies the unsealed body text of sealed emails.	Specify Text	string	none
EMAIL_SEALEDFORMAT Determines the format that sealed emails will be sent as.	Seal Format	0 = Microsoft Word 1 = RTF 2 = Plain Text	0

These settings relate to options on the Email tab of the Oracle IRM Desktop Options dialog, and on the Sealed Email Options dialog you can access by clicking the Settings button on the Email tab.

2.5.7 Authentication Settings

The authentication settings that you can preconfigure are as follows:

Property and description	UI Option	Values	Default
AUTHENTICATION_DISABLESAVECREDENTIALS Determines whether users can cache their authentication credentials. If caching is not allowed, users will have to enter their username and password whenever foreground synchronization to the Oracle IRM Server is required.	None	0 = allow caching option 1 = disable caching option	0
AUTHENTICATION_ SUPPRESSPRIVACYPOLICYDIALOG Suppresses the dialog that allows users to read a server's policy on handling personal data. Normally, this dialog appears before first contact with any new server, and a user must accept the policy before using Oracle IRM. This dialog should only be suppressed at sites which have a known, fixed list of Oracle IRM Servers, and where the users have been informed of the privacy policy by other means.	None	0 = show dialog normally 1 = never show dialog	0

2.5.8 Legacy Setting

The term "Legacy" refers to earlier releases of Oracle IRM Server, specifically 10*g*. The legacy setting that you can preconfigure is as follows:

Property and description	UI option	Values	Default
LEGACY_SHOWAUTHENTICATIONMENU Determines whether the drop-down menu for authentication types is shown.	Synchronization Messages	0 = do not show 1 = show	1

This setting relates to the authentication dialog that is shown for legacy servers.

2.5.9 Local Data Clean-Up Setting

This setting is read both on install and uninstall.

The local data clean-up setting that you can preconfigure is as follows:

Property and description	UI option	Values	Default
LOCALDATA_CLEAN Determines whether a local data clean-up is performed and, if so, whether it is a safe clean or a full clean. A safe clean: ■ deletes `HKEY_CURRENT_USER\Software\Oracle\IRM` ■ moves `C:\Documents and Settings\<user>\Local Settings\Application Data\Oracle\IRM folder` (on Windows XP) or `C:\Users\<user>\AppData\LocalLow\Oracle\IRM` (on Windows Vista) to the recycle bin **for all users** ■ moves `C:\Documents and Settings\All Users\Application Data\Oracle\IRM` (on Windows XP) or `C:\ProgramData\Oracle\IRM` (on Windows Vista) to the recycle bin A full clean performs all the operations of a safe clean, plus the following: ■ deletes `HKEY_LOCAL_MACHINE\Software\Oracle\IRM\StoreSecurity` (the machine key)	None	0 = no action 1 = safe clean 2 = full clean	0

2.5.10 Oracle IRM Background Process Startup Setting

The Oracle IRM background process startup setting that you can preconfigure is as follows:

Property and description	UI option	Values	Default
STARTIRMBACKGROUND Determines whether `IrmBackground.exe` starts automatically at the end of the installation. If set to 1, `IrmBackground.exe` automatically starts for the logged in user at the end of the installation. If set to 0, `IrmBackground.exe` will start on login, so it is advisable to reboot the machine to make this happen.	None	0 = do not start 1 = automatically start	1

2.5.11 Extracting the MSI File from the Self-Extracting Executable

If you prefer to use the MSI file directly, you can extract it as follows:

1. On a test box, run the Oracle IRM Desktop installation executable, but click Cancel on the first installation screen.

   Runing the executable extracts the MSI file to a subfolder of the current user's temporary area. For example:

   ```
   C:\Documents and Settings\Fred\local
   settings\temp\Oracle-IRM-Installer-NNN
   ```

where `NNN` is a number. This is a subfolder of the folder defined by the `%TEMP%` environment variable.

The equivalent location in Windows Vista and Windows 7 is:

```
C:\Users\Fred\AppData\Local\Temp\Oracle-IRM-Installer-NNN
```

2. Navigate to that folder and take a copy of the MSI file.

You can now use the MSI file for your corporate roll-out.

2.6 Registry Key Policy Setting

Oracle IRM Desktop looks for configuration settings in the following keys, in order:

1. HKLM\Software\Policies\Oracle\IRM (machine wide policy)
2. HKCU\Software\Policies\Oracle\IRM (user policy)
3. HKCU\Software\Oracle\IRM (user setting)
4. HKLM\Software\Oracle\IRM (default setting)

The installer can be used to set the default settings (4 above) by passing in installer parameters (as described in Section 2.5, "Silent and Unattended Installations").

A user can override these settings through the Oracle IRM Desktop Options dialog (3 above).

To lock settings so that they cannot be changed by users, the policy keys must be set by group policy (1 or 2 above). The sub key path, value name and type information required to set group policy is given in Section 9.5, "Registry Key Information".

2.7 Integrating Lotus Notes with Oracle IRM Desktop

This section contains the following topics:

- Introduction to Lotus Notes Integration
- Defining the Seal and Send Action
- Propagating the Mail Template Change to All Mail Databases
- Checking that the Lotus Notes Integration Works

2.7.1 Introduction to Lotus Notes Integration

These sections describe how to use the Lotus Domino Designer to integrate sealing options into a mail template on a Lotus Domino Server. The procedure applies to Domino 7 and might differ for other versions.

When you have completed the integration tasks, users will see a Seal on Send checkbox when composing new email.

When sending an email containing sensitive information, users simply need to tick the Seal on Send checkbox. When users are ready to send the email, they click the Send button as usual, and will be prompted to choose the appropriate context for the email. The email will be sealed to the selected context before being sent. If the email is ever forwarded, it will only be accessible to users who have rights in the context.

As a prerequisite for this procedure, you might need to load the Lotus Domino Designer application, which is not installed on the Domino Server by default.

If you do not integrate sealing options into your mail template, users can still access sealing options from menus. However, for ease of use and to encourage users to remember to seal email when appropriate, Oracle recommends that you integrate the options into your template as described here.

The process of integrating sealing options into a mail template comprises:

1. Adding a Seal on Send checkbox to a subform and propagating the changes to mail databases.
2. Checking that the integration works.

> **Note:** Oracle recommends that you make a backup copy of your mail template file before making changes, for example, `C:\Program Files\Lotus\Domino\Data\mail7.ntf`.

2.7.2 Defining the Seal and Send Action

Define the Seal and Send action as follows:

1. Start the Lotus Domino Designer application.
2. Choose **Open an Existing Database** and select the server to customize.
3. Select the relevant database, for example, Mail (R7), and click **Open**.
4. Expand the `Shared Code` folder and select `Subforms`.
5. Open the `DelOptionSubform` subform.
6. Make a copy of the `Encrypt` field that you can edit to create your Seal on Send checkbox. For example, create an `Encrypt_1` field.
7. Double-click the new field so that you can edit it as follows.
   a. Change the field name to `SMSealOnSend`.
   b. On the second tab, in the choices list box, enter `Seal on send|1`.
   c. On the sixth tab, amend the `Hide if` formula to ensure that the checkbox only appears for users who have Oracle IRM Desktop installed. You need to append the following to the formula:

      ```
      @Environment("SMSealAndSend") != "1"
      ```

      For example, the formula might now read:

      ```
      getCal := @GetProfileField("CalendarProfile";
      "showOptions"); From != @UserName |
      @IsAvailable($HideMailHeader) | getCal = "0" |
      @Environment("SMSealAndSend") != "1"
      ```
8. Save the changes.

2.7.3 Propagating the Mail Template Change to All Mail Databases

Having changed the mail template, the change needs to be propagated to all mail databases. Changes are usually scheduled to be propagated automatically at night. If you want to propagate the changes immediately, do the following:

1. Open a command prompt.
2. Go to the Domino installation folder, for example, `C:\Program Files\Lotus\Domino`.

3. Execute the following command:

```
ndesign -d mail
```

2.7.4 Checking that the Lotus Notes Integration Works

Having propagated the changes, you need to check that they work correctly. This involves using Lotus Notes on a computer that has Oracle IRM Desktop installed and that has the Lotus Notes integration enabled. It also involves having the right to create sealed email, which means that you need to have a Contributor role in at least one context.

Use the following procedure to check that the Lotus Notes integration works:

1. Close any open Lotus Notes windows and enable Lotus Notes integration in Oracle IRM Desktop (by checking the **Lotus Notes** box on the Email tab of the Oracle IRM Desktop Options dialog).
2. Start Lotus Notes and send a test memo to yourself.
3. Expose the suboptions of the memo, and check that the Seal on Send checkbox is present.
4. Check the **Seal on Send** checkbox, then click **Send**.

   You should be prompted to select a context for the memo. If no contexts are listed, use the **Refresh Available Contexts** option. When you receive the memo, you should find that it is sealed.
5. Finally, use another computer to check that the Seal on Send checkbox is exposed only to users who have Oracle IRM Desktop installed and the Notes integration option enabled.

2.8 Installing Oracle IRM Desktop in a Citrix Environment

This document describes how to deploy Oracle IRM Desktop for users of Citrix environments. It also provides guidance on how to control rights synchronization for Citrix users.

This installation allows in-application sealing of documents (that is, sealing within Microsoft Word, Excel, and PowerPoint).

Installing the Oracle IRM Desktop Software

In a Citrix environment, you need to install the Oracle IRM Desktop software on each Citrix server. You need to use the Windows Add/Remove Programs dialog rather than simply run the installation directly, as follows:

1. Obtain the Oracle IRM Desktop installation executable, and save it to a location accessible from the Citrix server, but do not run it.
2. Use the Windows Add Or Remove Programs application to install the Oracle IRM Desktop installation executable on the Citrix server.

Having installed the Oracle IRM Desktop software on each Citrix server, it is possible for Citrix users to start working with sealed documents according to their rights. However, Oracle recommends that you set up login and logout scripts to control rights synchronization in a non-standard way.

Note: If users are allowed to use non-Citrix systems as well as a Citrix system, you need to use device limits to ensure that rights are available on both types of system. For example, users might have laptops for mobile use as well as access to a Citrix system. By default, a user's rights can only be cached on one system at a time. An administrator can raise the device limit (which will apply to all users) as required. See *Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server*.

Controlling Rights Synchronization for Citrix Users

We recommend that you use scripts to control rights synchronization for Citrix users. This is the simplest way to ensure that rights will be available regardless of which Citrix server hosts a given session. Without such scripts, a user's rights might be cached on one server when the user is using another.

This guidance presumes that Citrix users are using Windows authentication to access sealed documents.

You might use the following HTML application (HTA) at the start of a user's Citrix session:

```
<html>
<head>
<script type=text/javascript>
function done(){
  close();
}
</script>
</head>
<body onLoad="done()">
<script type=text/javascript>
self.moveTo(2000,2000);
</script>
<OBJECT CLASSID="clsid:18CEFFD2-A724-11D3-B647-86BD54000000"
TYPE="application/login-softseal" TITLE="Retrieve Rights" WIDTH=150 HEIGHT=150
id=SealedMedia_Unsealer_Plugin1>
<PARAM NAME=server VALUE="https://servername:443/irm_desktop">
<PARAM NAME=refreshall VALUE="true">
</OBJECT>
</body>
</html>
```

The first `<PARAM>` tag specifies the address of your rights server. The second `<PARAM>` tag specifies the operation that you want to occur: `refreshall`. This synchronizes the user's rights so that they are available for the session.

A similar script with the `releaseall` parameter would run at the end of a session.

3

Getting Started with Oracle IRM Desktop

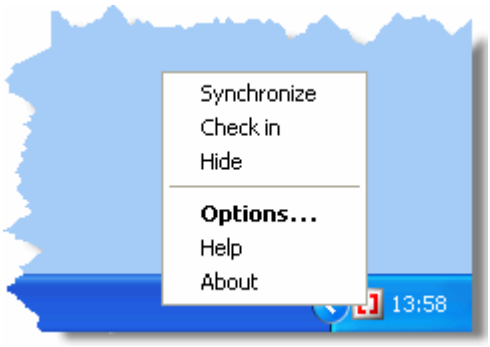
Note: If you share your machine with other users, please read Section 7.2, "Managing Rights on a Shared Computer".

This section describes how to use Oracle IRM Desktop for the following typical tasks:

- Opening Sealed Documents
- Sealing an Existing Document
- Creating a New Blank Sealed Microsoft Office Document
- Enabling Microsoft Office Integration

Microsoft Office integration provides sealing functionality on toolbars within the Microsoft Office applications you select.

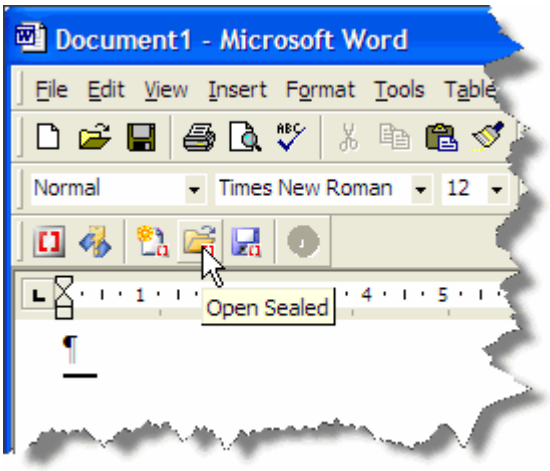
For information about other tasks, see the Oracle IRM Desktop online help. The help is accessible from the Windows Start menu, or from the Oracle IRM Desktop icon in the notification area (system tray).



3.1 Opening Sealed Documents

With Oracle IRM Desktop installed, you can open a sealed document simply by double-clicking it in a document browser (such as Windows Explorer).

Alternatively, with Microsoft Office integration enabled, you can use the toolbars within Microsoft Office applications.



The first time you open a sealed document, you might be challenged for the username and password of your Oracle IRM Server account, and you might be required to change your password. If you are challenged for a password, you might be offered a **Save my password** option, which you can use to ensure that you are not challenged next time.

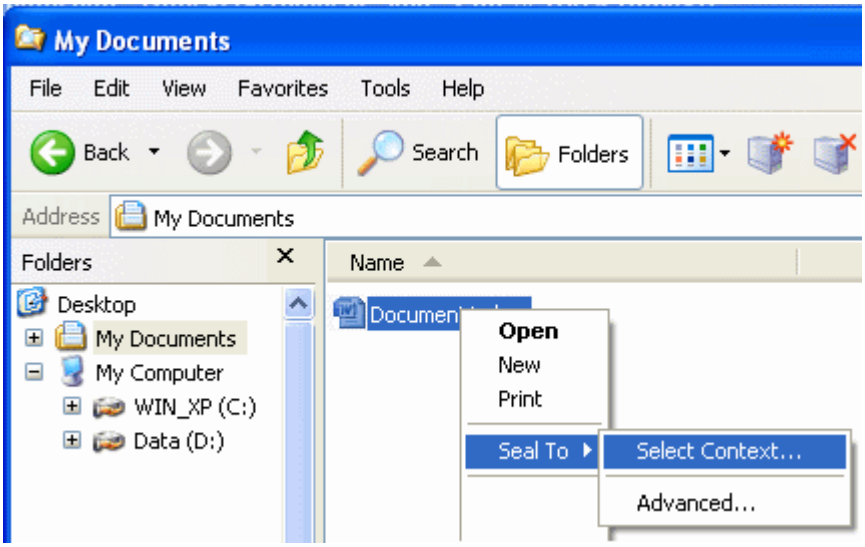
Having authenticated, the Oracle IRM software checks to see whether you have the right to open the sealed document. Typically, the administrator will make sure you have rights for the first document you receive. Once opened, your ability to interact with the document is controlled by your rights, and can range from read-only access, through the ability to add comments or make tracked changes, to full edit rights.

If you do not have the right to open the document, you are redirected to a web page that explains why not.

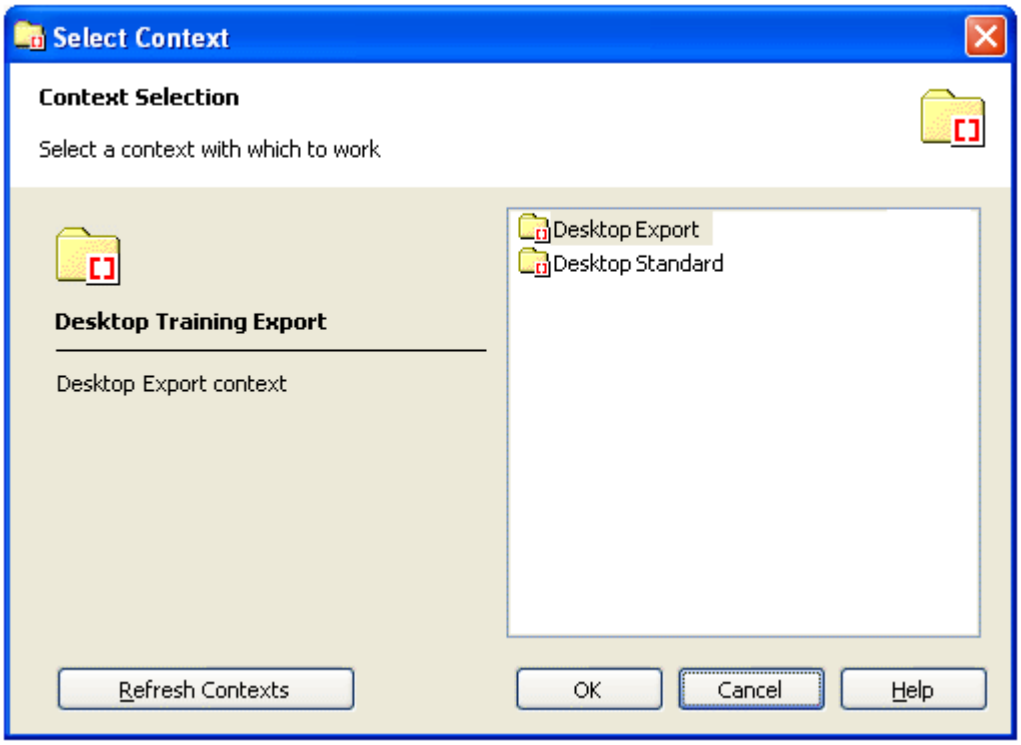
3.2 Sealing an Existing Document

You can seal an existing document in Windows Explorer as follows. The same procedure can seal Microsoft Word, Excel, Powerpoint, PDF, HTML, and various other document types.

1. Right-click on the document in Windows Explorer, select **Seal To** and then **Select Context**.



A context selection dialog appears:



The dialog lists security contexts to which you have the right to seal documents. If you think the list is incomplete, you can use the **Refresh Contexts** button to update it.

2. Select the context that you want to use and click **OK**.

   A sealed document is created in the same folder as the selected document.

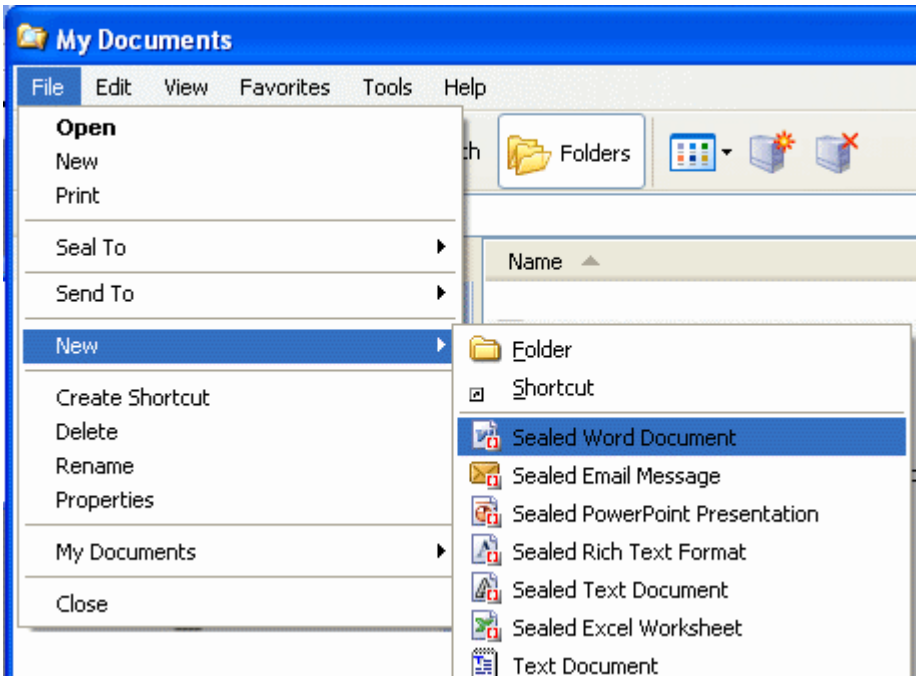
Alternatively, integrated Microsoft Office support provides sealing options within Microsoft Office applications. In each case, the option requires the selection of a context as shown above.

3.3 Creating a New Blank Sealed Microsoft Office Document

You can create new blank sealed Microsoft Office documents from the Windows Explorer File menu - just as you can create new unsealed documents.

For example, you can create a sealed Microsoft Word document, as follows:

1. In Windows Explorer, select the folder in which you want to create the new sealed document.
2. Select the **File** menu, then select **New**, then select **Sealed Word Document**.



The context selection dialog appears.

3. Select a context for the new sealed Word document and click **OK**.
4. Use the Save As dialog to name the new document.

   The new document is opened immediately for you to start working with.

Alternatively, Microsoft Office integration provides toolbars for creating new sealed documents within the Microsoft Office applications.

3.4 Enabling Microsoft Office Integration

If Microsoft Office integration is enabled, Oracle IRM Desktop supports the creation and editing of sealed Microsoft Office documents, and controls Microsoft Office to ensure that you do not accidentally exceed your rights. Microsoft Office integration might be enabled automatically. If not, you can enable it manually as follows.

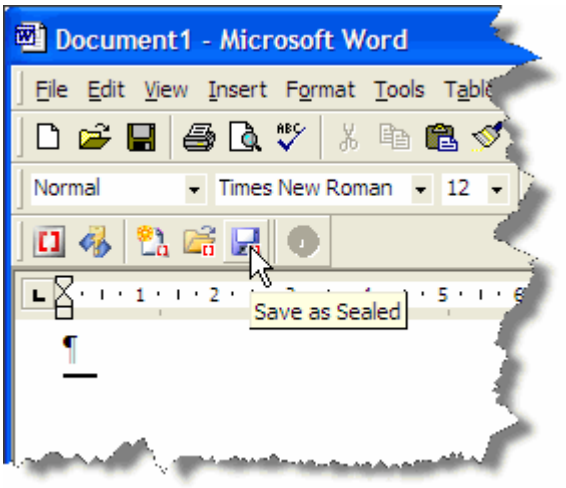
1. From the Windows Start menu, select Programs, then Oracle IRM Desktop, then Options.

   This opens the Oracle IRM Desktop Options dialog.

   Alternatively, you can right-click the Oracle IRM icon in the Windows notification area (system tray) and select Options.

2. Select the General tab.
3. If the Enable Microsoft Office support box is not already checked, check it, then click **OK**.

The next time you start a Microsoft Office application, it will show sealing-related options in an Oracle IRM toolbar. For example, you can use the Save As Sealed button on the Oracle IRM toolbar to seal a document:



Similar integrations for email applications are provided on the Email tab of the Oracle IRM Options dialog.

4

Working with Sealed Documents

This section covers the following topics:

- Opening Sealed Documents
- Editing Sealed Documents
- Creating New Sealed Documents
- Saving Changes to Sealed Documents
- Changing the Contexts That Documents are Sealed to
- Unsealing Sealed Documents
- Searching Sealed Documents
- Printing Sealed Documents
- Screen Capturing Sealed Documents
- Using Sealed Microsoft Excel Spreadsheets
- Using Sealed Microsoft Office Templates

4.1 Opening Sealed Documents

This section covers the following topics:

- About Opening Sealed Documents
- Opening a Sealed Document in a File Browser
- Opening a Sealed Document in a Microsoft Office Application

4.1.1 About Opening Sealed Documents

Your rights (see Section 1.3, "About Rights") determine whether you can open a sealed document, and what you are allowed to do with the document once it is open.

To open a document that has been sealed using Oracle IRM, you must have Oracle IRM Desktop installed on your computer.

4.1.2 Opening a Sealed Document in a File Browser

Rights: To open a sealed document, you need the Open right. See Section 1.3, "About Rights".

Microsoft Windows Explorer

Use one of the following procedures to open a document in Microsoft Windows Explorer:

- double-click the document name, or
- select the document name, then select **Open** from the **File** menu.

The Microsoft Desktop

Use one of the following procedures to open a document from the Microsoft Desktop:

- double-click the document icon on the Desktop, or
- right-click the document icon on the Desktop, then select **Open**.

Microsoft Internet Explorer

Use the following procedure to open a document that is listed on a page in Microsoft Internet Explorer:

1. Click the file name, or right-click the file name and select **Open**.
2. In the File Download dialog, select either **Open** (to immediately open the sealed file in its associated application), or **Save** (to save the sealed file to a location from which it can be opened later).

Protected View: You cannot use the **Open** option in the File Download dialog if the sealed file is a Microsoft Office document and Microsoft Office is configured to use "Protected View" (a Microsoft Office 2010 feature). In this case, use the **Save** option.

4.1.3 Opening a Sealed Document in a Microsoft Office Application

---

Rights: To open a sealed document, you need the Open right. See Section 1.3, "About Rights".

If you have enabled Microsoft Office support (see Section 3.4, "Enabling Microsoft Office Integration" and Section A.1.1, "General Tab"), you can use the Oracle IRM Desktop toolbar to open a sealed document.

Use the following procedure to open a sealed document in a Microsoft Office application:

1. Open the Microsoft Office application.
2. On the Oracle IRM Desktop toolbar, click the **Open Sealed** button.

   This opens the Open Sealed dialog, which lists sealed documents of the type shown in the Files Of Type drop-down list.
3. In the Files Of Type drop-down list, select the type of sealed file to open (for example, Sealed Word Document).
4. In the files area, select the sealed file to open.
5. Click **Open**.

You can also open sealed documents in the same way as other documents. For example, you can click the Open button in the Microsoft Word toolbar, and then select a sealed document from the familiar Open dialog. In this case, you can use the All

Files option in the Files Of Type drop-down list to show any type of file, whether sealed or not.

4.2 Editing Sealed Documents

This section covers the following topics:

- About Editing Sealed Documents
- About Using the Clipboard while Editing Sealed Documents

4.2.1 About Editing Sealed Documents

If you have sufficient rights, as explained below, you can make changes to (edit) sealed documents in the same way and for the same reasons that you would make changes to unsealed documents.

As a prerequisite to editing a sealed document, you need the Open right. See Section 1.3, "About Rights". You will also need at least one edit right, as described below:

- If you have been given the Edit right, you are able to edit a document as you would an unsealed document (unless other rights have been applied that restrict this). You may find that some application features have been restricted to increase document security.
- If you have been given the Edit Tracked right, you are able to edit a document, but the track changes option is automatically invoked. (Applies only to Microsoft Word documents.)
- If you have been given the Interact right, you are able to fill in form fields. If this is the only edit right you have been given, other types of edit are prevented.
- If you have been given the Screen Capture right, you are able to take screen captures.
- If you have been given the Program right, you are able to use macros that process or modify sealed content.

4.2.2 About Using the Clipboard while Editing Sealed Documents

If you have sufficient rights, as explained below, you can use the clipboard to move content from one document to another.

If you have been given the Edit right, you can use the clipboard to help you. However, your ability to paste information to another document is controlled by additional permissions set up on the server to which the sealed document is synchronized.

Depending on your permissions on the server:

- You might be allowed to paste within the same sealed document, but to no other document.
- You might be allowed to paste to a document of the same type, for example from one Microsoft Word document to another Microsoft Word document, but not from a Microsoft Word document to a Microsoft Excel spreadsheet.
- You might be allowed to paste anywhere you want, including to unsealed documents.

If you attempt to paste sealed content to an unauthorized destination, Oracle IRM Desktop displays a message explaining that you cannot.

Note: Copying and pasting from sealed HTML is always disabled regardless of your rights and permissions.

4.3 Creating New Sealed Documents

This section covers the following topics:

- About Creating New Sealed Documents
- Using Windows Explorer to Create a New Microsoft Office Document that is Sealed from the Outset
- Using Microsoft Office to Create a New Document that is Sealed from the Outset
- Creating a Sealed Version of an Existing Unsealed Document

4.3.1 About Creating New Sealed Documents

You can create a new sealed document in more than one way:

- For Microsoft Office documents, you can create a blank document that is sealed at the point of creation.
- For other document types, you must first create an unsealed document as you would normally, and then seal the document.

In both of the above cases, you create the sealed document either by using menu items in Windows Explorer, or by using the Oracle IRM toolbar within a Microsoft Office application. If you have unsealed documents as icons on your Microsoft Desktop, you can seal them using the icon's context menu. These options are explained in the sections that follow.

If you do not want unsealed versions of your sealed documents to exist, you may be able to set an Oracle IRM Desktop option that will remove the unsealed version when a sealed version is created. (See Section A.1.2, "Desktop Sealing Tab"). This option may already have been set (or disabled) by your system administrator.

4.3.2 Using Windows Explorer to Create a New Microsoft Office Document that is Sealed from the Outset

Rights: To seal a document, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to create a new document that is sealed from the outset:

1. In Windows Explorer, select the **File** menu and choose **New**, then choose the **Sealed** menu item for the document type that you want to create. For example, to create a new sealed Word document, choose **Sealed Word Document**.
2. In the Select Context dialog, select the context to which you want to seal the new document.

   If the context that you want to use is not shown, try refreshing the list by clicking the **Refresh Contexts** button.
3. Select a location and enter a name for the new document.

If more than one type of sealed file is available from the **Files of type** drop-down list, choose the type that you require.

If you have been authorized to allocate item codes manually (see Section 1.7, "About Sealed Document Item Codes"), you will see an Options section on the dialog for naming a document. To set the item code, check the **Update Item Code** box (if not already set), select the **Use This Item Code** option, then enter an item code in the accompanying text box.

4. Save the new document.

The new sealed document is opened in the appropriate application, if available. You can then work on the sealed document to the extent that your rights allow.

4.3.3 Using Microsoft Office to Create a New Document that is Sealed from the Outset

Rights: To seal a document, you need the Seal right. See Section 1.3, "About Rights".

If Microsoft Office support is enabled (this is an option on the General tab of the Oracle IRM Desktop Options dialog), use the following procedure to create a new document that is sealed from the outset:

1. In the Microsoft Office application, select the **New Sealed** icon on the Oracle IRM toolbar.
2. On the resultant menu, do one of the following:
   - select the context to which you want to seal the document, or
   - if the required context is not shown, select the **Select Context** menu item, or
   - if you want to base your new sealed document on a sealed template (in which the context will already have been set), select the **From Sealed Template** menu item.
3. If you have opened the Select Context dialog, select the context to which you want to seal the new document.

   If the context that you want to use is not shown, try refreshing the list by clicking the **Refresh Contexts** button.
4. If you have opened the Select Sealed Template dialog, select the sealed template on which you want to base your sealed document.

   You may have to change the type of template shown in the **Files of type** drop-down list to see the template that you want.
5. Select a location and enter a name for the new document.

   If more than one type of sealed file is available from the **Files of type** drop-down list, choose the type that you require.

   If you have been authorized to allocate item codes manually (see Section 1.7, "About Sealed Document Item Codes"), you will see an Options section on the dialog for naming a document. To set the item code, check the **Update Item Code** box (if not already set), select the **Use This Item Code** option, then enter an item code in the accompanying text box.
6. Save the new document.

The new sealed document is opened. You can then work on the sealed document to the extent that your rights allow.

4.3.4 Creating a Sealed Version of an Existing Unsealed Document

Rights: To seal a document, you need the Seal right. See Section 1.3, "About Rights".

Use one of the following procedures to create a sealed version of a document that already exists:

- In Windows Explorer, select the unsealed document, select the **File** menu, select **Seal To**, then select **Select Context**. In the Select Context dialog, select the context, then click **OK**.
- On your Microsoft Desktop, right-click the icon that represents the unsealed document, select **Seal To**, then select **Select Context**. In the Select Context dialog, select the context, then click **OK**.
- If Microsoft Office support is enabled, open the unsealed document in the Microsoft Office application and select the **Save As Sealed** button in the Oracle IRM toolbar.

If you have been authorized to allocate item codes manually (see Section 1.7, "About Sealed Document Item Codes"), you will see an Options section on the dialog for naming a document. To set the item code, check the **Update Item Code** box (if not already set), select the **Use This Item Code** option, then enter an item code in the accompanying text box.

4.4 Saving Changes to Sealed Documents

This section covers the following topics:

- About Saving Changes to Sealed Documents
- Saving Changes to A Sealed Document

4.4.1 About Saving Changes to Sealed Documents

If you have sufficient rights, you can save changes that you make to a sealed document.

It is very unlikely that you will have the right to edit a document but not the right to save changes. However, there are occasions when this might be the case. For example, you might have the right to change the values in a sealed Microsoft Excel worksheet so that you can plot charts for different scenarios and compare various projections, but you might not have the right to save changes to the worksheet.

Caution: When working with plain text files, be aware that any format changes or other operations you make that are not supported by the text file format will be lost when you save the file.

You may want to make changes to a sealed document but save the changes in an unsealed copy of the document. See Section 4.6, "Unsealing Sealed Documents".

4.4.2 Saving Changes to A Sealed Document

Rights: To save changes to a sealed document, you need the Reseal right. See Section 1.3, "About Rights".

Use the following procedure to save changes to a sealed document:

- Use the **Save** or **Save As** options as usual.

To save a copy of a document that is shown within Internet Explorer (for example, a PDF document), use Internet Explorer's **Save** (or **Save As**) option.

4.5 Changing the Contexts That Documents are Sealed to

This section covers the following topics:

- About Changing Contexts
- Changing the Context That a Document is Sealed To

4.5.1 About Changing Contexts

If you have sufficient rights, you can change the context that a document is sealed to. When doing this, you can choose to retain the original document (in a different location or with a different name), or you can overwrite the original sealed document.

During the lifecycle of a specific document, it might be appropriate for it to be sealed to different contexts at different times. For example, if you have a document sealed to a "work-in-progress" context (see Section 1.4, "About Contexts"), you might want to change it to a "published" context. Similarly, a document that is highly sensitive at the beginning of its lifecycle might become less sensitive after public announcements have been made.

4.5.2 Changing the Context That a Document is Sealed To

Rights: To change the context that a document is sealed to, you need the Copy To right for the current context and the Seal right for the destination context. See Section 1.3, "About Rights". You are limited to changing to certain trusted contexts. If there are any trusted contexts that you can change to, they are listed at the bottom of the Rights tab of the Oracle IRM Desktop Control Panel, in the Trusted Destinations section.

Use the following procedure to change the context to which a document is sealed:

1. Right-click the sealed document in Windows Explorer.

   If the sealed document is represented by an icon on your Microsoft Desktop, you can right-click that icon instead.

2. From the menu, select **Reseal To**.
3. In the Select Context dialog, select the context that you want to seal the new version to, then click **OK**.
4. Do one of the following:

- To create a copy of the document sealed to the new context, change the directory or the file name, then click **Save**.
- To replace the original document, click **Save**.

4.6 Unsealing Sealed Documents

This section covers the following topics:

- About Unsealing Sealed Documents
- Unsealing a Sealed Document

4.6.1 About Unsealing Sealed Documents

If you have sufficient rights, you can unseal a sealed document (that is, you can make an unsealed copy of a sealed document). The unsealed document can then be used without restrictions. The rights to do this are usually given only for relatively non-sensitive documents.

4.6.2 Unsealing a Sealed Document

Rights: To unseal a sealed document, you need the Save Unsealed right. See Section 1.3, "About Rights".

Use the following procedure to unseal a document:

1. Do one of the following:
   - Open the sealed document in its normal application and, from the **File** menu, select **Save As**.
   - Right-click the document in Windows Explorer and select **Unseal**.
   - Right-click the icon that represents the document on your Microsoft Desktop and select **Unseal**.
2. In the **Files of Type** drop-down box, select an unsealed file type.
3. If required, change the location and name of the document, then click **Save**.

4.7 Searching Sealed Documents

This section covers the following topics:

- About Searching Sealed Documents
- Enabling Sealed Documents to Be Searched
- Configuring for the Microsoft Indexing Service
- Configuring Search Logging

4.7.1 About Searching Sealed Documents

You can search sealed documents, subject to your rights, as follows:

- You can use the search facility provided within any application that displays a sealed document that you have the right to open. For example, you could use the search facility provided by Microsoft Word to search a sealed Word document that

you are viewing. This type of search does not require a specific right: you can search any sealed document that you can open.

- You can use the search facility in your operating system (for example, the Windows Explorer file manager in Microsoft Windows XP) to search folders that contain sealed documents. If you have the Search right, search results may then include matches in sealed documents as well as unsealed documents. To use this search facility, you must at least enable search within Oracle IRM Desktop (see Section 4.7.2, "Enabling Sealed Documents to Be Searched"). Additionally, for the Microsoft Windows 2008, Microsoft Vista, and Microsoft Windows 7 operating systems, you must also configure Oracle IRM Desktop for the Microsoft Indexing Service (see Section 4.7.3, "Configuring for the Microsoft Indexing Service").

  Note: If you do not configure Oracle IRM Desktop for the Microsoft Indexing Service, sealed documents may still be included in the results of a file search, but for the Microsoft Windows 2008, Microsoft Vista, and Microsoft Windows 7 operating systems, not all file locations will have been searched.

Search integration supports sealed Microsoft Office formats, sealed HTML, sealed XML, sealed email, and sealed PDF.

You will usually be given the Search right for any documents for which you have the Open right. However, you may be given only the Search right, in which case you will be able to search for the content of sealed documents but not open those documents.

Searching any PDF, including sealed PDF, requires a PDF filter. If the computer from which the search is implemented has Adobe Reader installed, it will probably already have the necessary filter. If the search is to be implemented from a computer that does not normally have Adobe Reader installed, the required filter is, at the time of writing, freely downloadable from Adobe.

Even if you are not using one of the operating systems that requires Oracle IRM Desktop to be configured for the Microsoft Indexing Service, it may still be useful to do so if your organization stores large numbers of sealed documents on a file share. Doing so will enable the Microsoft Indexing Service to create indexes that include sealed documents, and searches of the file share will then find sealed documents more efficiently.

4.7.2 Enabling Sealed Documents to Be Searched

Note: There are special procedures for enabling search within Microsoft SharePoint. See Section 8, "Using Oracle IRM Desktop with Microsoft SharePoint".

Sealed documents will be included in the results of any file search only if Oracle IRM Desktop is set to enable the searching of sealed documents. This applies to any Windows operating system.

Additionally, to include all file locations within the Microsoft Windows 2008, Microsoft Vista, and Microsoft Windows 7 operating systems, you must also configure Oracle IRM Desktop for the Microsoft Indexing Service. See Section 4.7.3, "Configuring for the Microsoft Indexing Service".

Use the following procedure to enable sealed documents to be searched:

1. Open the Oracle IRM Desktop Options dialog (for example, from the Windows Start menu, by selecting **Programs**, then **Oracle IRM Desktop**, then **Options**).
2. On the Search tab, make sure that the **Enable Search** box is checked.

4.7.3 Configuring for the Microsoft Indexing Service

You can configure the Oracle IRM Desktop search feature to use the Microsoft Indexing Service to support sealed documents.

Note: To include all file locations in searches within the Microsoft Windows 2008, Microsoft Vista, and Microsoft Windows 7 operating systems, you must configure Oracle IRM Desktop for the Microsoft Indexing Service.

Note: The Oracle IRM Desktop search feature can be used only with an account that uses basic authentication as the user authentication method. Other methods of user authentication, such as Windows Native Authentication (WNA) and forms authentication, cannot be used for the account.

Use the following procedure to configure Oracle IRM for the Microsoft Indexing Service:

1. Open the Oracle IRM Desktop Options dialog (for example, from the Windows Start menu, by selecting **Programs**, then **Oracle IRM Desktop**, then **Options**).
2. On the Search tab, click **Advanced**.
3. On the Indexing Service Configuration dialog, click **New**.
4. On the Oracle IRM Server URL page, specify the address of the Oracle IRM Server that manages the rights for the sealed documents that you want to be able to index. You can find a list of addresses and port numbers on the Servers tab of the Oracle IRM Desktop Options dialog.

4.7.4 Configuring Search Logging

The Oracle IRM Desktop search service writes messages to the Windows event log to report the status of the sealed document search.

Use the following procedure to configure certain aspects of the search logging feature:

1. Open the Oracle IRM Desktop Options dialog (for example, from the Windows Start menu, by selecting **Programs**, then **Oracle IRM Desktop**, then **Options**).
2. On the Search tab, click **Settings**.
3. On the Search Log Configuration dialog, select the message categories that you want written into the Windows event log, then click **OK**.

4.8 Printing Sealed Documents

This section covers the following topics:

- About Printing Sealed Documents
- Printing a Sealed Document

4.8.1 About Printing Sealed Documents

There are two print rights for sealed documents, the Print right and the Print To File right. See Section 1.3, "About Rights". If you have one of these rights for a specific sealed document, you can print it as if it were an unsealed document. If you do not have a print right for a document, the relevant print menu options and toolbars are disabled.

4.8.2 Printing a Sealed Document

Rights: To send a sealed document to a printer, you need the Print to File right or the Print right. To print a sealed document to a file, you need the Print to File right. The Print to File right includes the Print right. See Section 1.3, "About Rights".

Use the following procedure to print a sealed document:

1. Using the usual application for the document type, open the document that you want to print.
2. Use the usual method for printing a document. For example, select the **File** menu, then select **Print**.

4.9 Screen Capturing Sealed Documents

This section covers the following topics:

- About Screen Capturing Sealed Documents
- Sharing a Sealed Presentation During a Web Conference
- Capturing the Image of a Sealed Document

4.9.1 About Screen Capturing Sealed Documents

Oracle IRM Desktop controls your use of screen capture mechanisms, including the mechanisms used by popular web conferencing applications.

If you have the right to screen capture, then you can do so in the usual way.

If you do not have the right to screen capture, Oracle IRM Desktop uses an image to mask sealed documents when you invoke the capture operation.

4.9.2 Sharing a Sealed Presentation During a Web Conference

Rights: To start a web conference and share a sealed presentation, you need the Screen Capture right. See Section 1.3, "About Rights".

Use the following procedure to share a sealed presentation:

1. Start the web conference.
2. Share the sealed presentation as if it were an unsealed presentation.

If you do not have the Screen Capture right, remote observers will see a blanking image comprising numerous Oracle IRM logos.

4.9.3 Capturing the Image of a Sealed Document

> **Rights:** To capture the image of a sealed document from the screen, you need the Screen Capture right. See Section 1.3, "About Rights".

Use the following procedure to capture an image of a sealed document from the screen:

1. Capture the image in the usual way. For example, **Alt+PrintScreen**.
2. Paste the captured image into the destination application. For example, in Microsoft Word, select the point at which you want the image to be inserted, then select the **Edit** menu and select **Paste**.

If you do not have the Screen Capture right, an image comprising numerous Oracle IRM logos will be pasted into the destination application instead of the captured image.

4.10 Using Sealed Microsoft Excel Spreadsheets

This section covers the following topics:

- About Sealed Microsoft Excel Spreadsheets
- Linking Sealed Microsoft Excel Spreadsheets
- Updating Links Between Previously Unsealed Spreadsheets

4.10.1 About Sealed Microsoft Excel Spreadsheets

The Oracle IRM solution for opening, editing, creating, resealing, and searching sealed documents is as applicable to Microsoft Excel spreadsheets as it is to other Microsoft Office documents. What you are able to do with Microsoft Excel spreadsheets is determined by the usual sealed document rights, such as Open, Edit, Seal, and Search. See Section 1.3, "About Rights". Additionally, the Formulae right determines whether formulae (formulas) are revealed or concealed in sealed spreadsheets.

The ability to display content from one sealed workbook in the cells of another sealed workbook is supported. This is the facility in Microsoft Excel to set up a link between workbooks by copying data (using the **Copy** command on the **Edit** menu) from a cell in one workbook and then pasting it (using the **Paste Special** command on the **Edit** menu) into a cell in the other workbook.

Oracle IRM allows such links between workbooks only if both workbooks are sealed to the same context.

> **Note:** If the pasted content is derived from data in cells in the same document (for example, a chart created from nearby data cells), the pasted content will not show in the destination document.

Oracle IRM will prevent unauthorized access to data. This means that if a link is created to a sealed workbook from an unsealed one, or if the user of one sealed workbook is not authorized to see the content of a sealed workbook linked to it, the content of a linked cell will be shown as "#REF".

You can use Oracle IRM fields (see Section 6, "Working With Oracle IRM Fields and Watermarks") to help reinforce the confidential nature of a Microsoft Excel spreadsheet.

4.10.2 Linking Sealed Microsoft Excel Spreadsheets

Linking Microsoft Excel spreadsheets usually involves copying the contents of a cell in one spreadsheet and pasting it (using **Paste Special**) into the cell of another spreadsheet. This means that any changes made to the cell in the first spreadsheet will be reflected in the second spreadsheet.

However, to protect the cell content of sealed spreadsheets, there are restrictions on the use of **Copy** and **Paste Special** between separately opened Microsoft Excel workbooks: if you do not have copy rights (Copy or Copy To), the content will be pasted as fixed text, and not as text that will be updated when the source workbook changes.

4.10.3 Updating Links Between Previously Unsealed Spreadsheets

Caution: If you have existing unsealed spreadsheet files with links between them, seal **all** the files before updating the links between them. If you seal only the destination spreadsheet and then try to update the links to a pre-existing unsealed source, the links will be destroyed and will not be recoverable.

Rights: To open a sealed spreadsheet, you need the Open right. To seal a spreadsheet, you need the Seal right. To see formulas on a sealed spreadsheet, you need the Formulae right. See Section 1.3, "About Rights".

Use the following procedure to update existing links in spreadsheets that were previously unsealed:

1. Seal both the source and the destination spreadsheet files.
2. Open the sealed destination spreadsheet file.

   You will see the Microsoft Excel message telling you that there are links to other data sources.
3. Only if you have already sealed the source spreadsheet file, accept the option to update the links.

   You will see the Microsoft Excel message telling you that there are links that cannot be updated. (This is because the file extensions have been changed from `.xls` to `.sxls`.)
4. Accept the option to edit the links.

   You will see a list of links with the status `Error: Source not found`.
5. Use the dialog's change source facility to search for the sealed source file (with a `.sxls` extension).
6. If prompted to, log in to the sealed source file.

The links between the sealed spreadsheet files are re-established.

4.11 Using Sealed Microsoft Office Templates

This section covers the following topics:

- About Using Sealed Microsoft Office Templates
- Creating a Sealed Microsoft Office Template from Within Microsoft Office
- Creating a Sealed Microsoft Office Template Using Windows Explorer
- Editing Sealed Microsoft Office Templates

4.11.1 About Using Sealed Microsoft Office Templates

Sealed templates have the same benefits as ordinary templates: they enable you to create new documents in a simple and consistent way. However, when you use a sealed template, the new document is sealed to the same context as the template. For example, if a template is sealed to the Top Secret context, then all documents created from it are sealed to the Top Secret context too.

4.11.2 Creating a Sealed Microsoft Office Template from Within Microsoft Office

Rights: To open a sealed template or document, you need the Open right. To seal an unsealed template or document, you need the Seal right. To edit a sealed template, you need the Edit right, or an associated right. To save changes made to a sealed template, you need the Reseal right. See Section 1.3, "About Rights".

Use the following procedure to create a sealed template from within Microsoft Office (this uses Microsoft Word as an example):

1. Make sure that Microsoft Office integration is enabled:
   a. Right-click the Oracle IRM icon in the notification area (system tooltray) and select **Options**.
   b. On the Oracle IRM Desktop Options dialog, select the General tab.
   c. Make sure that the **Enable Microsoft Office support** checkbox is checked.
2. Open a Microsoft Word template that you want to seal, or open a Microsoft Word document that you want to save as a sealed template.
3. On the Oracle IRM toolbar, click the **Save as Sealed** icon.
4. Select a context for the sealed template.

   After selecting a context, Microsoft Office displays a dialog to enable you to name the file and specify its type.
5. From the **Files of type** drop-down list, select a sealed template type.

   For legacy Microsoft Office systems, select `*.sdot`. For Microsoft Office 2007, select `*.sdotx` or `*.sdotm`, as appropriate.
6. Specify an appropriate name and location for the template, and save it.

   The document is saved as a sealed template, and immediately opened with Oracle IRM Desktop for you to continue editing if required.

4.11.3 Creating a Sealed Microsoft Office Template Using Windows Explorer

Rights: To seal an unsealed template, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to create a sealed template using Windows Explorer:

1. In Windows Explorer, select an unsealed template (for example, `.dot`, `.dotx`, `.dotm`, `.xlt`, or `.pot`).
2. Right-click the selected template.
3. Select **Seal To** and the context that you want documents created from this template to be associated with.

4.11.4 Editing Sealed Microsoft Office Templates

Rights: To open a sealed template, you need the Open right. To edit a sealed template, you need the Edit right, or an associated right. To save changes to a sealed template, you need the Reseal right. See Section 1.3, "About Rights".

Use one of the following procedures to edit an existing sealed template:

- In Windows Explorer, select the sealed template, select the **File** menu, select **Open**, edit the document, then save it.
- While using the relevant Microsoft Office application, select the **File** menu, then select **Open**. You can then use the **Files of Type** field on the Open dialog to specify that you want to open a sealed template. Edit the document, then save it.

5

Using Sealed Email

This section covers the following topics:

- Creating and Sending Sealed Email
- Opening Sealed Email Messages and Sealed Attachments
- Creating Sealed Email Replies
- Forwarding Sealed Email

5.1 Creating and Sending Sealed Email

This section covers the following topics:

- About Creating and Sending Sealed Email
- Creating and Sending Sealed Email using an Integrated Email Application
- Creating and Sending Sealed Email using an Existing Document Attachment
- Creating and Sending Sealed Email using Sealed Email Document Format

5.1.1 About Creating and Sending Sealed Email

> **Note:** The recipient of a sealed email will be able to read it only if he has Oracle IRM Desktop installed on his computer and he has been given sufficient rights. It is recommended that you insure intended recipients have Oracle IRM Desktop installed or know how to obtain it, especially if you send emails outside your own organization.

There are two main ways to create sealed email, subject to your rights and the software that you have installed on your system:

- If you use Microsoft Outlook or Lotus Notes, Oracle IRM sealing options can be integrated directly into your email application. You can mark an email to be sealed as it is sent. This allows the very easy sealing of new emails, replies, and forwarded emails. Replying and forwarding of sealed emails are handled very much like regular replying and forwarding, enabling you to participate in email threads where all the messages are sealed.
- You can use any email application to send any sealed document as an attachment. The attachment can be any sealed document, including one that has been created specially as a sealed email document using the facility added to Windows Explorer. The advantage of using the special sealed email document format is that

your message will look and behave more like a regular email for any recipients who use Oracle IRM Desktop with email integration enabled.

5.1.2 Creating and Sending Sealed Email using an Integrated Email Application

Rights: To create a new sealed email and send it, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to create and send sealed email using an integrated email application (Microsoft Outlook or Lotus Notes):

1. Enable integration with your email application by doing the following:
   a. Open the Oracle IRM Desktop Options dialog (either from the Windows Start menu or from the Oracle IRM icon in the notification area).
   b. Select the Email tab.
   c. Select the checkbox against the name of your email application, then click **OK**.

   Note: Integration with Lotus Notes must have been previously set up in accordance with Section 2.7, "Integrating Lotus Notes with Oracle IRM Desktop".
2. In your email application, click the **New Sealed Email** button.
3. In the message creation window of your email application, make sure that the **Seal on Send** button is in the pressed down position.
4. Write your email and go to send it in the usual way. You will be asked to select a sealing context before the message is sent.

5.1.3 Creating and Sending Sealed Email using an Existing Document Attachment

Rights: To seal a document, and to send it by sealed email, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to send sealed email using an existing document that contains the information to be sent:

1. If the document to be sent is unsealed, seal it in the usual way.
2. In your email application, create a message, attach the sealed document, and send it in the usual way.

5.1.4 Creating and Sending Sealed Email using Sealed Email Document Format

Rights: To create and edit a document in sealed email format, you need the Seal right and the Reply right. To send a sealed email using the integrated email applications, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to create and send a sealed email using an attachment in the sealed email document format:

1. Open Windows Explorer, select the **File** menu, select **New**, then select **Sealed Email Message**.
2. In the Context Selection dialog, select the context in which the message will be sealed.
3. In the Save As dialog, select the name and location for the sealed document. Make sure that the **Open new sealed document** box is checked.

   If you have been authorized to allocate item codes manually (see Section 1.7, "About Sealed Document Item Codes"), you will see an Options section on the dialog for naming a document. To set the item code, check the **Update Item Code** box (if not already set), select the **Use This Item Code** option, then enter an item code in the accompanying text box.
4. Write the message into the document application that is opened (usually Microsoft Word).
5. Save and close the document.
6. In your email application, create a message, attach the sealed document, and send it in the usual way.

5.2 Opening Sealed Email Messages and Sealed Attachments

Sealed Email Messages

Rights: To open a sealed email message, you need the Open right. See Section 1.3, "About Rights".

A sealed email message always reaches the recipient as an attachment to a regular email. The file format of the attachment will be Microsoft Word, rich text, or plain text, depending on how Oracle IRM was configured by the sender.

Use one of the following procedures to open a sealed email message:

- In the email application, open the attached sealed message in the same way that you would open a regular attachment.

  Note: If the email message was sent in Microsoft Word format and you are using Microsoft Outlook with "Protected View" turned on, you will not be able to open the message in Outlook. Instead, you may be able to open the message as described in the alternate procedure below. ("Protected View" is a Microsoft Office 2010 feature.)

- Save the attached sealed message locally (for example, to your Windows Desktop), then open it from there.

Sealed Attachments

> **Rights:** To open a sealed file that has been sent as an attachment to an email, you need the Open right for that file. See Section 1.3, "About Rights".

The sender may have sent you an email with a sealed file attached. The sealed file may be in any of the formats supported by Oracle IRM.

Use one of the following procedures to open a sealed file that has been sent as an attachment:

- In the email application, open the sealed attachment in the same way that you would open a regular attachment.

  > **Note:** If the attachment is in a sealed Microsoft Office format and you are using Microsoft Outlook with "Protected View" turned on, you will not be able to open the attachment in Outlook. Instead, you may be able to open the message as described in the alternate procedure below. ("Protected View" is a Microsoft Office 2010 feature.)

- Save the sealed attachment locally (for example, to your Windows Desktop), then open it from there.

5.3 Creating Sealed Email Replies

Using the integrated email applications, you can create sealed replies to unsealed emails, and you can reply to sealed emails to create sealed email threads.

This section covers the following topics:

- Creating a Sealed Reply to an Unsealed Message
- Replying to a Sealed Email

5.3.1 Creating a Sealed Reply to an Unsealed Message

> **Rights:** To create a sealed reply to an unsealed email message, you need the Seal right. See Section 1.3, "About Rights".

Use the following procedure to create a sealed reply to an unsealed email message:

1. In your email application, click the **Reply** button.
2. In the message creation window, make sure that the **Seal on Send** button is in the pressed down position.
3. Write your reply and go to send it in the usual way. You will be asked to select a sealing context before the reply is sent.

5.3.2 Replying to a Sealed Email

> **Rights:** To reply to a sealed email, you need the Reply right or the Reply Tracked right. To save changes that you make to a sealed email, you need the Reseal right. See Section 1.3, "About Rights".

Use the following procedure to reply to a sealed email (that is, an email with a sealed attachment):

1. In your email application, open the sealed email attachment.
2. Click the Oracle IRM **Reply** button or **Reply to All** button.
3. In the document application that is opened, write your reply.

   The original sealed text will be visible in the document application, and will be indented, as will the text of any subsequent sealed replies.
4. Choose one of the following options:
   - To save the reply text and send it immediately, click the **Send Now** button.
   - To save the reply text and attach it to an outgoing email, ready for sending later, click the **Save and Attach** button.

The reply will be sealed to the same context as the original sealed email.

5.4 Forwarding Sealed Email

Using the integrated email applications, you have a choice of ways to forward sealed email.

This section covers the following topics:

- Forwarding Sealed Email Without Amendment
- Forwarding Sealed Email With Amendments
- Sealing and Forwarding an Email that was Received Unsealed

5.4.1 Forwarding Sealed Email Without Amendment

> **Rights:** To forward a sealed email without amendment, you do not need any rights. See Section 1.3, "About Rights".

Use the following procedure to circulate a sealed email to other recipients (this uses Microsoft Outlook as an example):

1. Select or open the sealed email.
2. Click **Forward**.

   Outlook creates an email so that you can specify the addresses that you want to forward it to. The sealed email is displayed as an attachment.
3. Specify the recipients.
4. Click **Send**.

The message is forwarded to the specified recipients with its sealed attachment unaltered. The recipients can open the sealed attachment subject to their rights, as usual.

5.4.2 Forwarding Sealed Email With Amendments

Rights: To forward a sealed email with amendments, you need a Reply right and the Reseal right. See Section 1.3, "About Rights".

Use the following procedure to add some comments to a sealed email before forwarding it to other recipients (this uses Microsoft Outlook as an example):

1. Open the message and open its sealed attachment.

   Outlook opens a window to display the sealed attachment. This window is read-only (just as regular email windows are read-only).

2. Click **Forward** in the window of the sealed attachment.

   Outlook creates a new window to display an editable version of the sealed attachment (just as it opens a new, editable window when you click **Forward** on a regular message).

3. Edit the sealed email as required.

   The original sealed email message is indented, just as Microsoft Outlook usually indents forwarded messages in email threads. You can add some text to the top of the message, or amend the text of the original message, as usual.

4. When ready, click **Save and Attach**.

Microsoft Outlook attaches the amended message to an email that you can address and send as usual.

5.4.3 Sealing and Forwarding an Email that was Received Unsealed

Rights: To seal and forward an email that was received unsealed, you need the Seal right. See Section 1.3, "About Rights".

This option is useful if someone sends you a message that you think should be sealed, or if you want to add some confidential remarks to a message before forwarding it.

Use this procedure to forward and seal an email that you received unsealed (this uses Microsoft Outlook as an example):

1. With the unsealed message open or selected, click **Forward**.
2. In the message editing window, click the **Seal on Send** button at any time before sending the message.
3. When you have finished adding any additional text and inserted the addressees, send the message (select the **File** menu and select **Send**).
4. From the Select Context dialog, select a context and click **OK**.

The original unsealed message is fowarded as a sealed attachment to the email.

6

Working With Oracle IRM Fields and Watermarks

This section covers the following topics:

- About Oracle IRM Fields and Watermarks
- Adding Oracle IRM Fields in Microsoft Word
- Adding Oracle IRM Fields in Microsoft Excel

6.1 About Oracle IRM Fields and Watermarks

Oracle IRM fields are placeholders for information about a sealed document, for example the name of the user who sealed the document, or the context to which the document is sealed. You insert Oracle IRM fields into documents before or after they are sealed. When Oracle IRM Desktop opens a sealed document that contains an Oracle IRM field, it transforms the field into the relevant item of information.

A document can contain many Oracle IRM fields. For a list of all the Oracle IRM fields, see Section 9.1, "List of Oracle IRM Fields".

A common use for Oracle IRM fields is to create watermarks in sealed documents. The watermarks will show on all instances of the sealed document. This can be used, for example, to help trace the origin of a sealed document that has been printed.

6.2 Adding Oracle IRM Fields in Microsoft Word

This section covers the following topics:

- Adding an Oracle IRM Field to a Microsoft Word Document
- Registering Oracle IRM Fields as Microsoft Word Document Properties
- Using Oracle IRM Fields That Have Been Registered As Microsoft Word Document Properties

6.2.1 Adding an Oracle IRM Field to a Microsoft Word Document

For typical uses of Oracle IRM fields, see Section 6.1, "About Oracle IRM Fields and Watermarks".

You can add fields anywhere in an unsealed Microsoft Word document. However, if you add them to headers and footers, they are repeated consistently on every page of a document, and can be used as a watermark that lies behind the main content of the page.

Rights: To complete this procedure you will need the Seal right, and to see transformed fields in sealed documents you will need the Open right as a minimum. See Section 1.3, "About Rights".

Use the following procedure to add an Oracle IRM Field to a Microsoft Word document:

1. Open an unsealed Microsoft Word document and position the cursor in the document to indicate where you want the field to appear.
2. Select the **Insert** menu, then select **Field**.
3. Select **Document Information** from the list of categories. (In Word 2007/2010, select **Quick Parts** in the Text area, then select **Field**.)
4. Select **DocProperty** from the list of field names. (In Word 2007/2010, click **Field Codes**.)
5. Edit the text field beneath the two lists so that it identifies the Oracle IRM field you want to use. (In Word 2007/2010, edit the **Field Codes** text box.) For example:

   ```
   DOCPROPERTY "irm-account-name"
   ```

   For the complete list of Oracle IRM fields, see Section 9.1, "List of Oracle IRM Fields".
6. Click **OK**.

   The string **Error! Unknown document property name** appears at the cursor. This is not a problem, but can be avoided as described in Section 6.2.2, "Registering Oracle IRM Fields as Microsoft Word Document Properties".
7. Save and close the Microsoft Word document.
8. Seal the Microsoft Word document.

When you open the sealed Microsoft Word document, the Oracle IRM field is transformed.

6.2.2 Registering Oracle IRM Fields as Microsoft Word Document Properties

You can simplify the use of Oracle IRM fields by registering them as Microsoft Word document properties. This procedure can be used to avoid an unhelpful error message being shown as a placeholder for the field data, as described in Section 6.2.1, "Adding an Oracle IRM Field to a Microsoft Word Document".

Rights: This procedure does not require any Oracle IRM rights.

Use the following procedure to register a field as a document property:

1. Open an unsealed Microsoft Word document.
2. Select the **File** menu, then select **Properties**.
3. Select the **Custom** tab.
4. Type the name of an Oracle IRM field, for example, irm-account-name.

   For the complete list of Oracle IRM fields, see Section 9.1, "List of Oracle IRM Fields".

5. Specify a value, for example, `"This field will be updated when sealed"`.
6. Click **OK**.

6.2.3 Using Oracle IRM Fields That Have Been Registered As Microsoft Word Document Properties

Having registered the field, it is available as an option next time you use the Field item on the Insert menu. The specified value appears in the Word document instead of the placeholder string.

> **Rights:** To complete this procedure you will need the Seal right, and to see transformed fields in sealed documents you will need the Open right as a minimum. See Section 1.3, "About Rights".

Use the following procedure to use a registered Oracle IRM field:

1. Open an unsealed Microsoft Word document and position the cursor in the document to indicate where you want the field to appear.
2. Select the **Insert** menu, then select **Field**.
3. Select **Document Information** from the list of categories.
4. Select **DocProperty** from the list of field names.
5. Click the **Options** button, select the Oracle IRM field from the list of properties, then click the **Add to Field** button.
6. Click **OK** to close the Field Options dialog.
7. Click **OK** to close the main Field dialog.

   The value of the field appears at the cursor.
8. Save and close the Microsoft Word document.
9. Seal the Microsoft Word document.

When you open the sealed Microsoft Word document, the field is transformed.

6.3 Adding Oracle IRM Fields in Microsoft Excel

> **Rights:** To complete this procedure you will need the Seal right, and to see transformed fields in sealed documents you will need the Open right as a minimum. See Section 1.3, "About Rights".

> **Note:** This procedure applies only to content sealed against 11*g* versions of Oracle IRM Server.

Use the following procedure to add an Oracle IRM field to a cell on a Microsoft Excel spreedsheet:

1. Open the Microsoft Excel spreadsheet and select the cell in which you want the field to appear.

2. Select the **Insert** menu, then select **Function**.
3. From the Function category list, select **Oracle IRM Add-in**.
4. From the Function name list, select **OracleIRM_CustomProp**.
5. Click **OK**.
6. In the Name box of the entry panel, enter the full field name.

   For example, to insert the field irm-account-name, enter `irm-account-name`.

   For the complete list of Oracle IRM fields, see Section 9.1, "List of Oracle IRM Fields".
7. Click **OK**.
8. Seal the Microsoft Excel document.

7

Managing Oracle IRM Rights

This section covers the following topics:

- About Obtaining and Managing Your Rights
- Managing Rights on a Shared Computer
- Connecting to Oracle IRM Server Manually
- Synchronizing Your Rights Manually
- Checking In Your Rights Manually
- Clearing Your Password

7.1 About Obtaining and Managing Your Rights

After initial connection to Oracle IRM Server, managing your rights is almost completely automatic.

When you attempt to open a sealed document that you have obtained or been sent, the Oracle IRM client software automatically contacts Oracle IRM Server to obtain your rights. If you have sufficient rights, you will be able to use the sealed document.

After you have established a connection to Oracle IRM Server, you may, if you have sufficient rights, be able to create new documents sealed to a context on that server. If you have not already connected to Oracle IRM Server (for example, by opening a document that someone else has sealed to that server), you will have to connect to the server manually (see Section 7.3, "Connecting to Oracle IRM Server Manually").

> **Note:** Because Oracle IRM Server will store data that allows you to be personally identified, on first contact with the server you will see a dialog asking you to confirm that you have read and accept the privacy policy associated with the sealed document. To use the sealed document, you must accept the privacy policy. You can cancel at this stage, in which case the document will not be shown, and no information about you will be stored on the server. This applies to 11*g* servers only and differs from previous releases of Oracle IRM.

Depending on how Oracle IRM has been configured, you might be prompted for your Oracle IRM credentials (user name and password).

Having requested your rights for the specific document you wanted to open, the software also sets up periodic rights synchronization. This automatic process means that you typically have all of your rights available to you even if Oracle IRM Server is temporarily unavailable. This enables you to work offline without further preparation.

(The length of time that you can work offline is set by the Oracle IRM Server domain administrator on a per role basis.)

> **Note:** For offline working, you will never be asked for a username and password when accessing a sealed document. This is because authentication for offline working is based on your Windows login.

In some circumstances, you might want to manage your rights manually. For example:

- If you are about to disconnect from the network and you want to be sure that your cached rights are as up-to-date as possible, you can synchronize manually.
- If you want to change the computer on which you are using sealed documents (for example, to work on a home PC), you may need to check in your rights to Oracle IRM Server. This is because a right can be used from only one computer at a time, unless Oracle IRM Server has been specifically configured to allow the use of multiple computers. When you check in, any open documents using your rights are closed. Another computer can then synchronize to the server, with the same account, and obtain those rights.
- If you have finished working at a computer that is shared by other users, you should consider checking in your rights manually.

7.2 Managing Rights on a Shared Computer

Each Oracle IRM Desktop user should log on to the computer using their own Microsoft Windows account.

If you are using a computer that is shared with others:

- before use, switch the Microsoft Windows account to your own, or log off and log on again as yourself
- after use, log off of your Microsoft Windows account before allowing anyone else to use the computer

If multiple Oracle IRM Desktop users obtain rights for content while logged on to a single Microsoft Windows account, the rights become merged, and anyone logged on to that account will have access to all users' content. If it is absolutely unavoidable for users to share a Microsoft Windows account, each user must check in their rights manually before allowing someone else to use the computer. See Section 7.5, "Checking In Your Rights Manually".

7.3 Connecting to Oracle IRM Server Manually

The easiest way to connect to Oracle IRM Server is to open a document that has already been sealed to a context on that server. If this is not possible, you will have to connect to the server manually.

Use the following procedure to connect to Oracle IRM Server manually:

1. From the Windows Start menu, select **Programs**, then **Oracle IRM Desktop**, then **Options**.

   This opens the Oracle IRM Desktop Options dialog.

   Alternatively, you can right-click the Oracle IRM icon in the notification area (system tray) and select **Options**.

2. On the Servers tab, select **New**.
3. On the Add Server dialog, enter the URL of the server.

   For connection to an 11*g* server, the URL will be in the form `https://servername:port/irm_desktop`. You should obtain the exact URL from the administrator of the server. The `/irm_desktop` extension is required.

   For connection to a 10*g* server, the URL will be in the form `seal://servername:80`.
4. To check that the connection can be made, select **Validate**.
5. To connect to the server, select **OK**.

If the connection details are valid, the server will be added to the list on the Servers tab.

7.4 Synchronizing Your Rights Manually

> **Note:** By following this procedure, your rights will be synchronized on servers where the Update Rights box is checked on the Servers tab of the Oracle IRM Desktop Options dialog. If there are servers that you do not want to synchronize with, uncheck the box on the Servers tab first.

Use the following procedure to synchronize your rights manually:

1. From the Windows Start menu, select **Programs**, then **Oracle IRM Desktop**, then **Synchronization and Check In**.

   This opens the Oracle IRM Desktop Options dialog.
2. On the Update Rights tab, select **Synchronize**.

Alternatively, you can right-click the Oracle IRM icon in the Windows notification area (system tray) and select **Synchronize**.

7.5 Checking In Your Rights Manually

> **Note:** By following this procedure, your rights will be checked in on servers where the Update Rights box is checked on the Servers tab of the Oracle IRM Desktop Options dialog. If there are servers that you do not want to check your rights into, uncheck the box on the Servers tab first.

You may need to check in your rights manually, for example:

- when you want to move to another computer and continue to use sealed documents
- after you have finished using sealed documents on a shared computer.

Use the following procedure to check in your rights manually:

- Right-click the Oracle IRM icon in the Windows notification area (system tray) and select **Check In**.

Alternatively, from the Windows Start menu, select **Programs**, then **Oracle IRM Desktop**, then **Synchronization and Check In**. Then, in the Oracle IRM Desktop Options dialog, select the Update Rights tab and select **Check In**.

You will be prompted to provide your authentication credentials (user name and password). This information is required to identify whose rights are being checked in: the departing user's credentials must be provided, not those of an arriving user.

7.6 Clearing Your Password

You will need to clear your password if you have more than one user identity on the server and you wish to change from one identity to another (perhaps because the different identities have different document access rights associated with them). This is applicable only if you were asked to select the **Remember My Password** checkbox on the Oracle IRM Server Credentials dialog and you did so.

Use the following procedure to clear your password:

1. From the Windows Start menu, select **Programs**, then **Oracle IRM Desktop**, then **Options**.

   This opens the Oracle IRM Desktop Options dialog.

   Alternatively, you can right-click the Oracle IRM icon in the notification area (system tray) and select **Options**.

2. On the Servers tab, check the **Update Rights** box against each server for which you want to clear the password. (The box may already be checked.)

3. Select **Clear Password**.

   A message will be displayed to confirm that the stored password has been cleared.

After the password has been cleared, you will be prompted to supply a username and password the next time that you need to contact the server, for example when opening a sealed document.

8

Using Oracle IRM Desktop with Microsoft SharePoint

This section covers the following topics:

- Using Sealed Documents With Microsoft SharePoint
- Modifying a Microsoft SharePoint Server for Use with Oracle IRM
- Enabling Search With Microsoft Sharepoint 2007

8.1 Using Sealed Documents With Microsoft SharePoint

This section describes how Oracle IRM Desktop supports Microsoft SharePoint in various versions of Microsoft Office.

See the *Release Notes* for any late variations to the levels of support described in this section.

Microsoft Office 2000 and Microsoft Office XP

For these versions of Microsoft Office, sealed files in Microsoft SharePoint are opened read-only, regardless of user rights.

To edit the file, copy it to your local file system (for example, the My Documents folder of Windows Desktop), make your changes, save the file, then upload it to Microsoft SharePoint.

Microsoft Office 2003 and Later

For these versions of Microsoft Office, sealed files in Microsoft SharePoint will open as editable if you have sufficient rights (and if the Microsoft SharePoint server has been modified for use with Oracle IRM), except in the following cases:

- the file has been locked by another user;
- you have only restricted rights to modify the sealed file, such as Annotate or Edit Tracked;
- you are using Microsoft Office 2010 to open documents with the formats `.sdocx`, `.sdocm`, `.sdotx`, or `.sdotm` from SharePoint 2010.

In these cases, the sealed file will open read-only. To edit a file that has been opened read-only, copy it to your local file system (for example, the My Documents folder of Windows Desktop), make your changes, save the file, then upload it to Microsoft SharePoint.

See Section 1.3, "About Rights".

8.2 Modifying a Microsoft SharePoint Server for Use with Oracle IRM

To modify a Microsoft SharePoint server so that it can handle sealed content:

1. Install a set of icon images to represent sealed content.

   The icon images are currently available from the Oracle Technology Network at the following location:

   http://www.oracle.com/technetwork/middleware/content-management/irm-fileicons-180493.zip

   Copy the images into the SharePoint `images` folder. In SharePoint 2007, this is:

   ```
   C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\IMAGES
   ```

2. Modify the `docicon.xml` file to add the sealed content types.

   In SharePoint 2007, the `docicon.xml` file is in the following location:

   ```
   C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\XML
   ```

   At the end of the section headed `<ByExtension>`, add the following lines:

   ```
   <Mapping Key="scsv" Value="icsxls.gif" EditText="Microsoft Office Excel"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdoc" Value="icsdoc.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdocm" Value="icsdoc.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdocx" Value="icsdoc.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdot" Value="icsdot.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdotm" Value="icsdot.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sdotx" Value="icsdot.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="spot" Value="icspot.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="spotm" Value="icspot.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="spotx" Value="icspot.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sppt" Value="icsppt.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="spptm" Value="icsppt.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="spptx" Value="icsppt.gif" EditText="Microsoft Office PowerPoint"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="srtf" Value="icsrtf.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="stxt" Value="icstxt.gif" EditText="Microsoft Office Word"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sxls" Value="icsxls.gif" EditText="Microsoft Office Excel"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sxlsm" Value="icsxls.gif" EditText="Microsoft Office Excel"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sxlsx" Value="icsxls.gif" EditText="Microsoft Office Excel"
   OpenControl="OracleIRM.OpenDocuments" />
   <Mapping Key="sxlt" Value="icsxlt.gif" EditText="Microsoft Office Excel"
   OpenControl="OracleIRM.OpenDocuments" />
   ```

```
<Mapping Key="sxltm" Value="icsxlt.gif" EditText="Microsoft Office Excel"
OpenControl="OracleIRM.OpenDocuments" />
<Mapping Key="sxltx" Value="icsxlt.gif" EditText="Microsoft Office Excel"
OpenControl="OracleIRM.OpenDocuments" />
<Mapping Key="seml" Value="icseml.gif" EditText="Microsoft Office Word"
OpenControl="OracleIRM.OpenDocuments" />
```

3. Modify the `htmltransinfo.xml` file to add the sealed content types.

   In SharePoint 2007, the `htmltransinfo.xml` file is in the following location:

   `C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\XML`

   At the end of the section headed `XML`, after any other file extension entries, add the following lines:

```
<Mapping Extension="scsv" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdoc" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdocm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdocx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdot" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdotm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sdotx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="spot" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="spotm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="spotx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sppt" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="spptm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="spptx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="stxt" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxls" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxlsm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxlsx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxlt" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxltm" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="sxltx" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="srtf" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
<Mapping Extension="seml" AcceptHeader="" HandlerUrl=""
ProgId="OracleIRM.OpenDocuments" />
```

4. Restart IIS.

8.3 Enabling Search With Microsoft Sharepoint 2007

Note: Search cannot currently be enabled for other versions of Microsoft SharePoint.

To enable searching of files with Sharepoint 2007, you need to do all of the following:

- Install Oracle IRM Desktop on the Microsoft SharePoint server.
- Enable file searching in Oracle IRM Desktop.

  See Section 4.7.2, "Enabling Sealed Documents to Be Searched".
- Configure Oracle IRM Desktop for the Microsoft Indexing Service.

  See Section 4.7.3, "Configuring for the Microsoft Indexing Service".
- Reconfigure the `OracleIRMServiceHost` service to support searching, as described below.

Reconfiguring the OracleIRMServiceHost Service to Support Searching

To reconfigure the `OracleIRMServiceHost` service to support searching:

1. Run DCOMCNFG.EXE (for example, by entering `dcomcnfg` into the Windows Run dialog and clicking **OK**).
2. Navigate to Component Services, Computers, My Computer, DCOM Config, OracleIRMServiceHost.
3. Right click and select **Properties** on OracleIRMServiceHost object.
4. Navigate to the Security tab in the OracleIRMServiceHost Properties dialog.
5. On the Security tab, in the Launch and Activation Permissions section, check the **Customize** check box and then click the **Edit** button
6. In the Launch and Activation Permission dialog, click the **Add** button to open the user selection dialog.
7. Add **Everyone** to the object names.
8. In the Launch and Activation Permission dialog, select the **Everyone** group name, then check the **Local Launch** and **Local Activation** check boxes.
9. On the Security tab, in the **Access Permissions** section, check the **Customize** check box, then click the **Edit** button.
10. In the Access Permission dialog, click the **Add** button to open the user selection dialog.
11. Add **Everyone** to the object names.
12. In the Access Permission dialog, select the **Everyone** group name, then check the **Local Access** check box.

Follow these steps to restart the `OracleIRMServiceHost` service with the new DCOM settings:

1. Start the service management console (for example, by entering `services.msc` into the Windows Run dialog and clicking **OK**).

2. Find the `OracleIRMServiceHost` service in the list of services.
3. Right-click `OracleIRMServiceHost` and select **Restart**.

9

Oracle IRM Desktop Reference

This section covers the following topics:

- List of Oracle IRM Fields
- Frequently Asked Questions
- Troubleshooting
- Formats
- Registry Key Information

9.1 List of Oracle IRM Fields

> **Note:** The fields listed in this section are for use only with content sealed against 11*g* versions of Oracle IRM Server. For content sealed against 10*g* versions of Oracle IRM Server, fields must continue to be inserted as described in the 10*g* user documentation. The former `SealedMedia_` and `OracleIRM_` name prefixes will continue to be recognized for the foreseeable future for use with 10*g* content.

The Oracle IRM solution supports a number of fields that you can add to documents before sealing them. When Oracle IRM Desktop opens a document that contains an Oracle IRM field, it transforms the field into the relevant item of information. A document can contain many Oracle IRM fields.

Typically, the following two fields provide a sufficient reminder of the sensitive nature of a document, and the user responsible for opening a specific copy:

- irm-account-name
- irm-classification-name

The complete list of Oracle IRM fields that you can consider using is as follows:

- irm-time

  All fields that end with -time will show Coordinated Universal Time (UTC).

- irm-time-local

  All fields that end with -time-local will show the local time, with the number of hours ahead or behind UTC included in parentheses.

- irm-locale
- irm-location

- irm-mime
- irm-extension
- irm-account-uuid
- irm-account-name
- irm-creation-time
- irm-creation-time-local
- irm-edit-time
- irm-edit-time-local
- irm-schema-version
- irm-classification-name
- irm-classification-description
- irm-classification-xml
- irm-classification-keyset
- irm-classification-system
- irm-classification-time
- irm-classification-time-local
- irm-classification-uri
- irm-host
- irm-context-itemcode-value
- irm-context-itemcode-time
- irm-context-itemcode-time-local
- irm-context-uuid

9.2 Frequently Asked Questions

This section covers the following topics:

- I have been prompted to log in manually, and I have forgotten my credentials. What do I do?
- I have logged in successfully but Oracle IRM Desktop says I do not have the rights to access a document. What do I do?
- When I log in I get a "Cannot connect to server" message. What do I do?
- I had a sealed document open and it just disappeared. What's happened?
- I am no longer able to edit the document I am working with. What's happened?
- I have two sealed documents from the same originator, but I can access only one of them. Why?
- Why has my account been locked out?
- Why can't I work with sealed Microsoft Office documents in the same way I work with normal ones?
- How do I seal email messages and threads?

- How do I add distinctive watermarks and headers and footers to sealed documents?
- How do I save changes I have made to VB code in a sealed document?
- How does Oracle IRM handle and protect objects embedded in sealed Microsoft Office documents?

I have been prompted to log in manually, and I have forgotten my credentials. What do I do?

If you have access to a password reset page, browse to that page and use it to reset your password. Otherwise, contact an Oracle IRM Server administrator for assistance.

I have logged in successfully but Oracle IRM Desktop says I do not have the rights to access a document. What do I do?

Oracle IRM Desktop usually redirects you to a web page that provides contact details for the person who can give you the rights you need. Contact that person and explain which document you are trying to open, and why you need access to it. They will decide whether it is appropriate to give you any rights.

If you see a message saying that your rights are already checked out to another computer, you need to check in your rights from that computer, or wait for the rights to expire.

When I log in I get a "Cannot connect to server" message. What do I do?

If you cannot connect to the server (Oracle IRM Server), there may be a problem with your network connection. If you connect to the Internet from a corporate network, you may need assistance from your network administrator to resolve the problem. Use the Oracle IRM Server Connection Test dialog to diagnose the problem. (Open this dialog from the Test link on the page that reported the error.)

If you see this message for only some documents, but can open others, then it is possible that you are being served by multiple Oracle IRM servers, one of which is temporarily unavailable.

I had a sealed document open and it just disappeared. What's happened?

Your rights have expired and you have been redirected to a web page.

If you are working offline, then go online and try to open the document again. It is possible that your locally cached rights have expired and that more rights can be obtained as soon as you go online.

If your rights have expired permanently, then the web page should provide contact details for the administrators who are authorized to grant you more rights.

If you were editing a sealed document online when your rights expired or were revoked, you will lose any unsaved changes. If your rights were downgraded, or if your locally cached rights expired, you are given an opportunity to save changes.

I am no longer able to edit the document I am working with. What's happened?

This is rare, but it is possible that your rights have been reduced since you started working on the document. If you think this might be the case, contact the owner of the context to which the document is sealed.

I have two sealed documents from the same originator, but I can access only one of them. Why?

It is quite usual for documents to be sealed to different contexts even if they come from the same originator. For example, you might receive documents sealed to a "Company Confidential" context and others sealed to a "Board Matters" context. It is likely that your rights for these two contexts will be different, such that you can only open one, or you can open them both, but edit only one.

Why has my account been locked out?

As a security measure, the Oracle IRM Server administrator has configured an account lock-out policy that prevents anyone from trying to guess passwords. If your account has been locked out, it is possible that someone else has been trying to log in using your account. Depending on the lock-out policy, your account might become accessible again after a short period, or might need to be manually reset. Contact your Oracle IRM Server administrator for further information.

Why can't I work with sealed Microsoft Office documents in the same way I work with normal ones?

The purpose of sealing documents is to control who has access, and who has edit rights. Edit rights are fine-grained, so you might find that you cannot use all of the Microsoft Office features you are familiar with. For example, you might find that you cannot print a sealed document, or that you are prevented from pasting information from one sealed document to another, or that the track changes option is always on.

Oracle IRM's goal is that using sealed documents should be very similar to using unsealed documents, if you have the necessary set of rights. Where rights are granted, you should be able to do what you usually do in most cases. In some cases, the need to protect a document might mean that options you are familiar with need to be disabled because they provide security loopholes.

How do I seal email messages and threads?

See Section 5, "Using Sealed Email". To use sealed email to full advantage, you need to enable email integration in Oracle IRM Desktop.

How do I add distinctive watermarks and headers and footers to sealed documents?

See Section 6, "Working With Oracle IRM Fields and Watermarks".

How do I save changes I have made to VB code in a sealed document?

To maintain the security of the VB code, it is not possible to save your VB code changes directly in the sealed document.

Use the following procedure to save changes that you have made to VB code in a sealed document:

1. Select the container document for the VB code document that you have changed.
2. Select **Save** in the container document.

How does Oracle IRM handle and protect objects embedded in sealed Microsoft Office documents?

You can seal a Microsoft Office document that already contains an embedded object, but not insert a new object into an existing sealed document. If an object was present in the document before it was sealed, Oracle IRM prevents the object from being edited. This does not apply to the data in charts (within chart objects), which is

protected by Oracle IRM. Chart objects can be inserted into Microsoft Office documents, and full interaction with them is allowed.

Data stored as part of the embedded object inside a sealed file is fully protected by Oracle IRM. However, if the embedded object references external data (that is, data external to the sealed file, such as in a database or external files) Oracle IRM will only protect access to it from within the sealed file, and alternative methods of protecting the data for other ways of access must be provided.

9.3 Troubleshooting

This section covers the following topics:

- Proxy Issues
- Sealed Documents Block Screen Captures

9.3.1 Proxy Issues

Oracle IRM Desktop needs to be able to communicate with a rights server (Oracle IRM Server) so that you can open sealed documents.

Oracle IRM Desktop communicates with 10*g* versions of Oracle IRM Server using a secure, encrypted variant of the HTTP protocol used by web browsers. Your network configuration might prevent this protocol from reaching Oracle IRM Server. For 11*g* versions of Oracle IRM Server, standardized HTTPS communications are used.

There are two types of network configuration that can cause problems:

- **Proxy servers**

  Your network might require Oracle IRM Desktop communications to pass through a specific computer, known as a proxy server. If so, then your browser also needs to use a proxy server, and should already have the required proxy server settings. Oracle IRM Desktop uses the same settings, so proxy servers should not cause problems.

  However, if your Oracle IRM Desktop is failing to communicate with Oracle IRM Server, and Oracle IRM Desktop tests report that there is a proxy server, report the problem to your network administrator.

  The use of proxy servers with indexed search integration will be problematic and is not advised.

- **Firewalls**

  A firewall monitors all communications between your local network and remote networks, and prevents any communications that it considers a security risk. Oracle IRM Desktop uses standard web browsing protocol. If your firewall allows you to browse the world wide web, you should also be able to communicate with Oracle IRM Server.

  If browsing the web is not permitted, you need to talk to your network administrator to arrange to allow communications to Oracle IRM Server. The firewall needs to allow outbound connections to the Oracle IRM Server address and port, and allow responses to such connections.

  You can use the Oracle IRM Desktop test facility to find out what address and port Oracle IRM Desktop is trying to contact, and then configure the firewall to allow the communication to succeed.

9.3.2 Sealed Documents Block Screen Captures

If you attempt to make a screen capture when a sealed document is on screen, the captured image often shows the sealed document in the foreground even though the sealed document is really in the background. This can mean that the application you were trying to capture is hidden.

This is intended behavior that prevents sealed documents being captured through transparent foreground applications. See Section 4.9, "Screen Capturing Sealed Documents".

9.4 Formats

Sealed documents have file icons and extensions that are slightly different to their unsealed counterparts. The table below shows the icons and extensions for the supported types of sealed document.

File icon	Unsealed extension	Sealed extension	Sealed MIME type
	pdf	spdf	application/vnd.sealedmedia.softseal.pdf
	html | htm	stml	application/vnd.sealedmedia.softseal.html
	png	spng	image/vnd.sealed.png
	gif	sgif	image/vnd.sealedmedia.softseal.gif
	jpeg | jpg	sjpg	image/vnd.sealedmedia.softseal.jpeg
	doc	sdoc	application/vnd.sealed.doc
	ppt	sppt	application/vnd.sealed.ppt

File icon	Unsealed extension	Sealed extension	Sealed MIME type
	xls	sxls	application/vnd.sealed.xls
	dot	sdot	application/vnd.sealed.template
	xlt	sxlt	application/vnd.sealed.template
	pot	spot	application/vnd.sealed.template
	docx	sdocx	application/vnd.sealed.docx
	docm	sdocm	application/vnd.sealed.docm
	dotx	sdotx	application/vnd.sealed.dotx
	dotm	sdotm	application/vnd.sealed.dotm
	pptx	spptx	application/vnd.sealed.pptx
	pptm	spptm	application/vnd.sealed.pptm

File icon	Unsealed extension	Sealed extension	Sealed MIME type
	potx	spotx	application/vnd.sealed.potx
	potm	spotm	application/vnd.sealed.potm
	xlsx	sxlsx	application/vnd.sealed.xlsx
	xlsm	sxlsm	application/vnd.sealed.xlsm
	xltx	sxltx	application/vnd.sealed.xltx
	xltm	sxltm	application/vnd.sealed.xltm
	mov	smov	video/vnd.sealedmedia.softseal.mov
	mpeg | mpg	smp1	video/vnd.sealed.mpeg1
	mp4	smp4	video/vnd.sealed.mpeg4
	xml	sxml	application/vnd.sealed.xml

File icon	Unsealed extension	Sealed extension	Sealed MIME type
	txt	stxt	application/vnd.sealed.txt
	rtf	srtf	application/vnd.sealed.rtf
	csv	scsv	application/vnd.sealed.csv
	doc	seml	application/vnd.sealed.eml.doc
	rtf	seml	application/vnd.sealed.eml.rtf
	txt	seml	application/vnd.sealed.eml.txt

9.5 Registry Key Information

This information is useful to administrators who want to use group policy to prevent users from changing Oracle IRM Desktop configuration settings. See Section 2.6, "Registry Key Policy Setting".

Oracle IRM Desktop Settings

See Section 2.5.2, "Oracle IRM Desktop Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
ShowTrayIcon	\Unsealer\	DWORD
HideIEToolbars	\Unsealer\	DWORD
OfficeEnabled	\Unsealer\	DWORD
ShowIrmBar	\Unsealer\	DWORD
AllowOnlineStatusPage	\Unsealer\	DWORD
OpenCSVPolicy	\Unsealer\	DWORD

Desktop Sealing Settings

See Section 2.5.3, "Desktop Sealing Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
Activated	\DesktopSealer\	DWORD
DeleteSourceFiles	\DesktopSealer\	DWORD
ClassificationMruSize	\DesktopSealer\Recent	DWORD
OpenNewSealedFile	\DesktopSealer\	DWORD

Synchronization Manager Settings

See Section 2.5.4, "Synchronization Manager Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
InitialServers	\Sync\InitialServers	STRINGs
LockedServers	\Sync\LockedServers	STRINGs
AutoSyncEnabled	\Sync\	DWORD
DefaultRetry	\Sync\	STRING
DefaultCatchup	\Sync\	STRING
LogLevel	\Sync\	DWORD
ShowSuccessInfo	\Sync\	DWORD
ShowFailureInfo	\Sync\	DWORD

Search Settings

See Section 2.5.5, "Search Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
Enabled	\Search\	DWORD
ReportErrors	\Search\	DWORD
ReportWarnings	\Search\	DWORD
ReportInformation	\Search\	DWORD

Email Settings

See Section 2.5.6, "Email Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
OutlookActivated	\Email\	DWORD
GroupWiseActivated	\Email\	DWORD
DisplayCloseSEMLWarning	\Email\	DWORD
DisplaySendAttachmentsWarning	\Email\	DWORD

Value name	Sub key path	Type
DisplayInvalidFormatWarning	\Email\	DWORD
BodyFile	\Email\Options\Body	STRING
EmailBodyType	\Email\Options\Body	DWORD
PlainTextBody	\Email\Options\Body	STRING
IndentReply	\Email\Options\Reply	DWORD
FontCharSet	\Email\Options\Reply\Font	DWORD
FontEffects	\Email\Options\Reply\Font	DWORD
FontFaceName	\Email\Options\Reply\Font	STRING
FontHeight	\Email\Options\Reply\Font	DWORD
FontMask	\Email\Options\Reply\Font	DWORD
FontOffset	\Email\Options\Reply\Font	DWORD
FontPitchAndFamily	\Email\Options\Reply\Font	DWORD
FontTextColor	\Email\Options\Reply\Font	DWORD
SealedEmailFormat	\Email\Options\SealFormat	DWORD
SignatureOnNew	\Email\Options\Signature	DWORD
SignatureOnReply	\Email\Options\Signature	DWORD
UseCustomTemplate	\Email\Options\Template	DWORD
TemplateFile	\Email\Options\Template	STRING

Authentication Settings

See Section 2.5.7, "Authentication Settings" for possible values for these properties (and other related information).

Value name	Sub key path	Type
DisableSaveCredentials	\Authentication\	DWORD
SuppressPrivacyPolicyDialog	\Authentication\	DWORD

Legacy Settings

See Section 2.5.8, "Legacy Setting" for possible values for these properties (and other related information).

Value name	Sub key path	Type
ShowAuthenticationMenu	\Legacy\	DWORD
DataDirectory	\Legacy\	STRING

Local Data Clean-Up Settings

See Section 2.5.9, "Local Data Clean-Up Setting" for possible values for these properties (and other related information).

Value name	Sub key path	Type
Clean	\LocalData\	DWORD

Value name	Sub key path	Type
CleanCurrentUser	\LocalData\	DWORD

A

User Interface

This section contains information about the user interface for Oracle IRM Desktop. The following features are described in this appendix:

- Oracle IRM Desktop Options Dialog
- Sealed Email Options Dialog
- Oracle IRM Desktop Control Panel Dialog
- General Features
- Oracle IRM Desktop Toolbars

A.1 Oracle IRM Desktop Options Dialog

The following tabs and dialogs are used to set options in Oracle IRM Desktop:

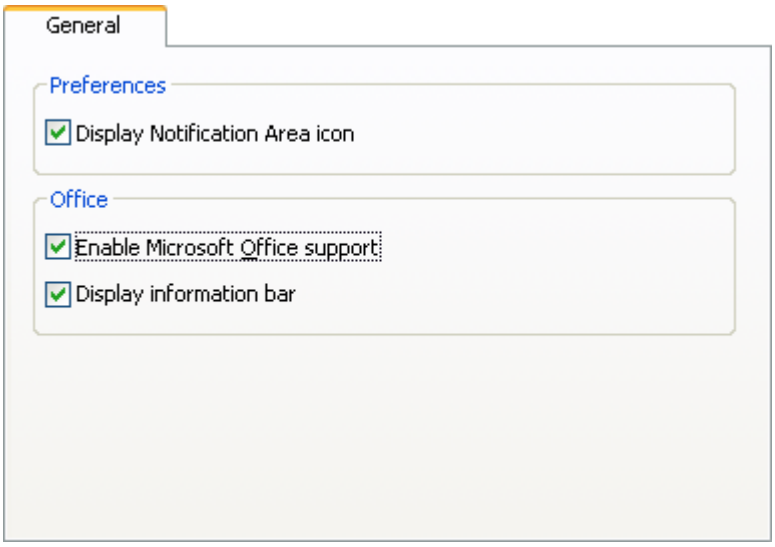
- General Tab
- Desktop Sealing Tab
- Servers Tab
- Update Rights Tab
- Search Tab
- Email Tab
- About Tab
- Add Server Dialog
- Search Log Configuration Dialog
- Synchronization Log Configuration Dialog
- Indexing Service Configuration Dialog

Open the Oracle IRM Desktop Options dialog by right-clicking the **Oracle IRM** icon in the system tooltray and selecting **Options**, or by opening the Microsoft Windows Control Panel and double-clicking the **Oracle IRM Desktop Options** icon.

A.1.1 General Tab

Use the General tab for setting the main preferences.

Open the tab by selecting **General** on the Oracle IRM Desktop Options dialog.



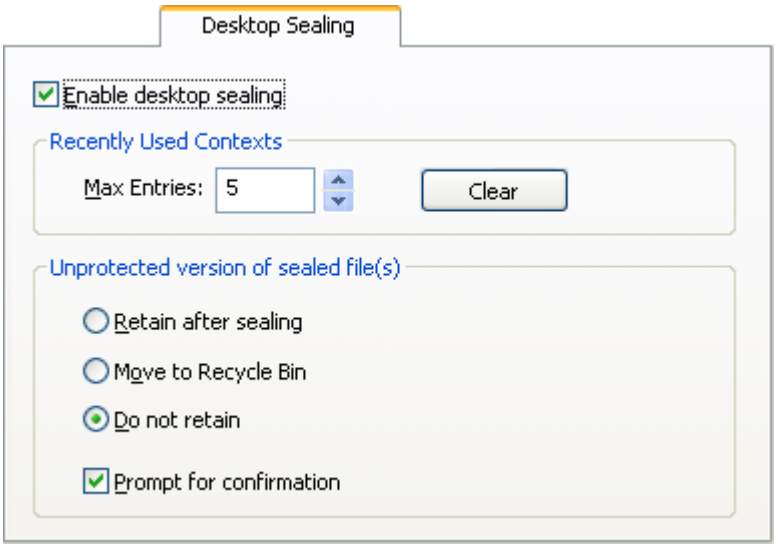
Element	Description
Display Notification Area icon (checkbox)	Normally checked. Unless you are a Citrix user, uncheck to remove the Oracle IRM icon from the row of icons in the bottom right corner of the screen. When double-clicked, this icon opens the Oracle IRM Desktop options dialog. You can also open this dialog from the Windows Control Panel. Citrix users must not uncheck this box.
Enable Microsoft Office support (checkbox)	Normally checked. Uncheck to disable the integration of sealing options directly into your Microsoft Office applications. Unchecking this option disables the opening of sealed Microsoft Office files.
Display information bar (checkbox)	Normally checked. Uncheck to never show the Oracle IRM messages area in Microsoft Office documents. If checked, the information bar for a specific document can be closed by clicking the black cross on the right of the bar in that document.

A.1.2 Desktop Sealing Tab

The desktop sealing feature integrates Oracle IRM sealing options into Windows Explorer:

- **Seal To**, **Reseal To** and **Unseal** options are added to the **File** menu.
- Options to create new sealed documents are added to the **New** submenu.
- Oracle IRM information is added to the file properties available through Windows Explorer. If you select a file and open its Properties dialog, there is an Oracle IRM tab that shows, for example, which context the document is sealed to.
- A pop-up description is displayed when you move your mouse pointer over the name of a sealed document (if Windows Explorer is configured to show such pop-ups).

Open the tab by selecting **Desktop Sealing** on the Oracle IRM Desktop Options dialog.

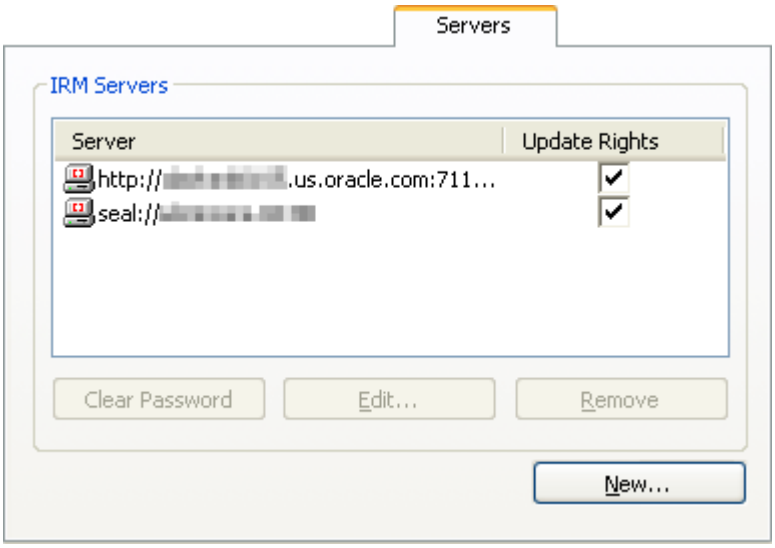


Element	Description
Enable desktop sealing (checkbox)	Normally checked. Uncheck to disable desktop sealing.
Recently Used Contexts	**Max Entries:** Default value is 5. Enter a number (between 0 and 20) to specify how many recently used contexts are offered when you use the Seal To and Reseal To menu options. When you seal or reseal a file, you need to specify which context you want to seal to. The recently used context list makes it easier to complete this task. Use the **Clear** button to remove the current value.
Unprotected version of sealed file(s)	Use to determine what happens to the original files when sealed versions of them are created. The default is that such files are retained in an unprotected state. **Retain after sealing:** The original files will not be removed after a sealed version has been created. The original files will be in an unprotected state. This is the default. **Move to Recycle Bin:** The original files will be moved to the Windows Recycle Bin after a sealed version has been created. The moved files can be recovered from the Windows Recycle Bin until the bin has been emptied. The file in the Windows Recycle Bin is in an unprotected state. If selected, the **Prompt for confirmation** checkbox becomes available and is unchecked. **Do not retain:** The original files will be removed after a sealed version has been created. This is a normal file system deletion, not a complete destruction of the file, so if you are concerned that this does not provide adequate security, you may want to consult your system administrator about further action. If selected, the **Prompt for confirmation** checkbox becomes available and is checked. **Prompt for confirmation:** Available if the **Move to Recycle Bin** option or the **Do not retain** option has been chosen. Select this checkbox if you want to see a prompt before an original file is deleted or moved after a sealed version has been created. The default status changes depending on which of the above options has been selected.

A.1.3 Servers Tab

The Servers tab shows a list of the servers to which sealed documents are or can be synchronized. Most of the time the list is managed automatically. In rare circumstances, you might add or remove a server manually. For example, if you know that your account has been deleted on a server, you can use the settings to remove the server from the list.

Open the tab by selecting **Servers** on the Oracle IRM Desktop options dialog.



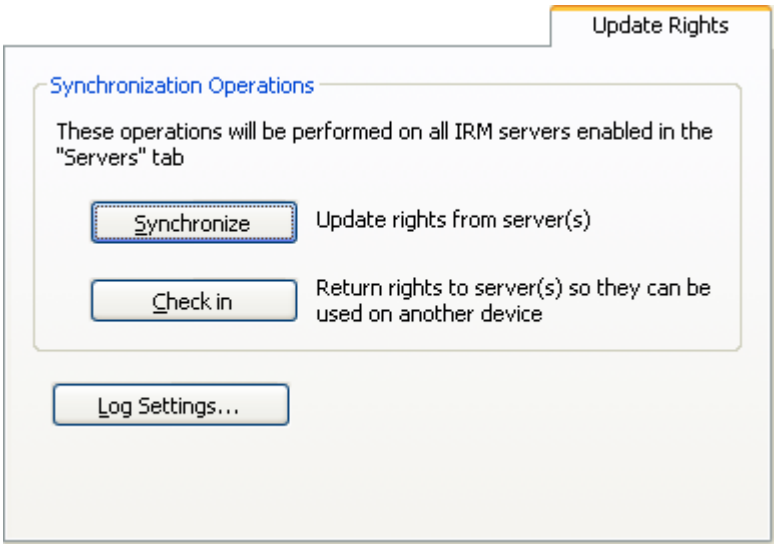
Item	Description
[Oracle] IRM Servers	Lists the servers that are available for your sealed documents to be synchronized with. **Server:** The address (URL) of the server. **Update Rights:** Normally checked. Any checked servers will be affected if you manually check in your rights. See Update Rights Tab. Uncheck a server if you do not want your rights to be checked in for that server. **Clear Password:** For the highlighted server, clears the stored username and password entered from this instance of Oracle IRM Desktop. You will need to clear the password if you have more than one user identity on the server and you wish to change from one identity to another (perhaps because the different identities have different document access rights associated with them). This is applicable only if you selected the Remember My Password checkbox on the Oracle IRM Server Credentials dialog. When you select the **Clear Password** button, you see a message that tells you either that the stored password has been cleared, or that no password is stored for the server. After the password has been cleared, you will be prompted to supply a username and password the next time that you need to contact the server, for example when opening a sealed document. **Edit:** Opens the Add Server Dialog, allowing you to change the URL of the item highlighted in the [Oracle] IRM Servers list. **Remove:** Removes the highlighted server from the list. There may be servers that cannot be removed, because of the way they have been configured. **New:** Opens the Add Server Dialog, through which you can add the URL of a server that you want added to the list.

A.1.4 Update Rights Tab

The Update Rights tab lets you synchronize your rights on remote servers with your locally cached rights. This tab also lets you give up your locally cached rights so that the server can reissue them to you on another device.

Your locally cached rights allow you to keep working with sealed documents even when you are disconnected from the network and cannot contact the server. Typically, your cached rights allow you to keep using documents for several days before being required to contact the server.

Open the tab by selecting **Update Rights** on the Oracle IRM Desktop options dialog.



Item	Description
Synchronize (button)	Updates the locally cached rights with those on the servers, where the Update Rights checkbox has been checked on the Servers tab.
Check in (button)	Gives up the locally cached rights for sealed documents managed by the servers whose Update Rights checkboxes have been checked on the Servers tab.
Log Settings (button)	Opens the Synchronization Log Configuration Dialog, through which you can select which synchronization message categories are written to the Windows event log.

A.1.5 Search Tab

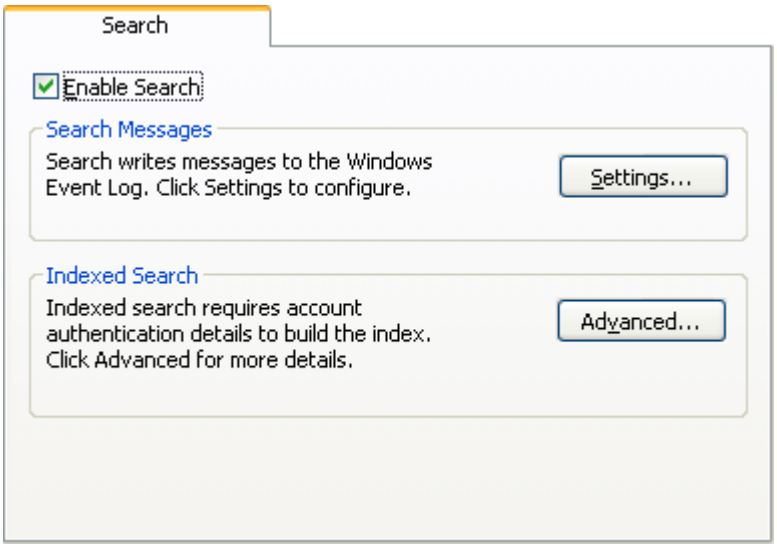
If enabled, searches of documents (in, for example, Windows Explorer) can find content in sealed documents that match the search criteria.

For the Microsoft Windows 2008, Windows Vista, and Windows 7 operating systems, the "advanced" indexed search facility must also be set up. If this is not done for these operating systems, the results of searches will exclude some file locations. For other operating systems, you do not need to set up the indexed search facility, although doing so will make searching more efficient.

Searches for content will attempt to match the search criteria in sealed documents as well as unsealed documents (presuming that you did not specify specific file types in which to search). The success of a search depends on whether you have the right to search the content of specific sealed documents in the folder. If the criteria are matched by content in a sealed document that you have the right to search, the sealed document is included in the search results.

You do not need to enable the search facility simply to search for the file names of sealed files.

Open the tab by selecting **Search** on the Oracle IRM Desktop Options dialog.



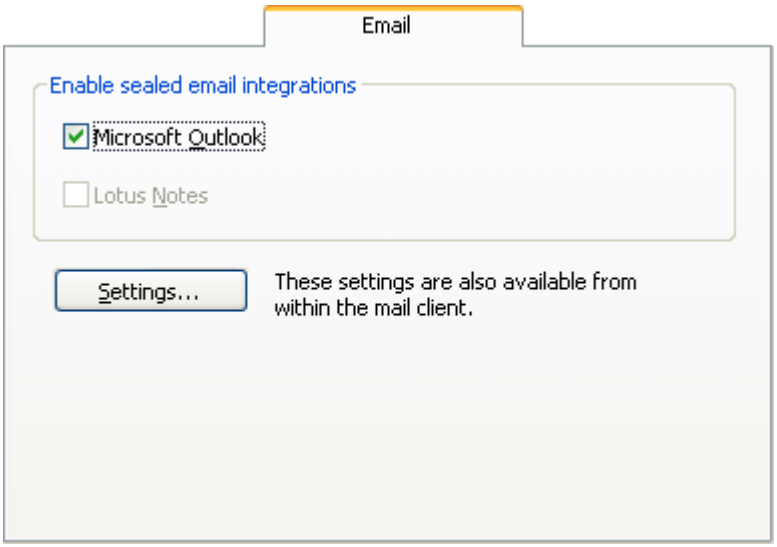
Item	Description
Enable Search (checkbox)	Normally checked. Uncheck if you do not want sealed documents to be included in the results of searches. Checking this box will enable the logging and indexing features described below.
Search Messages	If searching is enabled, searches generate a log showing the history of successful and unsuccessful searches involving sealed documents. (Unsuccessful searches are typically a result of not having the right to search.) **Settings:** Click to open the Search Log Configuration Dialog, through which you can choose whether the log is displayed, clear the contents of the log, view the log, and set the log location.
Indexed Search	You can configure the search component to enable the Microsoft Indexing Service to support sealed documents. Indexing can make searches more efficient, and is essential when searching within the Microsoft Windows 2008, Windows Vista, and Windows 7 operating systems. **Advanced:** Click to open the Indexing Service Configuration Dialog, through which you can add details for the Oracle IRM Servers that will handle the indexing.

A.1.6 Email Tab

The Oracle IRM Desktop email features integrate sealing options into the Microsoft Outlook or Lotus Notes mail clients. This enables you to create sealed messages and reply threads in those clients as easily as you can create regular email.

Users of other email clients can create and receive sealed email, but the option is not integrated into the mail client. Typically, you would select **New** from the **File** menu in Windows Explorer to create a new sealed message. You could then use the attachment functionality of any email client to send the sealed email message. Similarly, sealed email that you receive appears as an attachment that you open in the normal way.

Open the tab by selecting **Email** on the Oracle IRM Desktop options dialog.



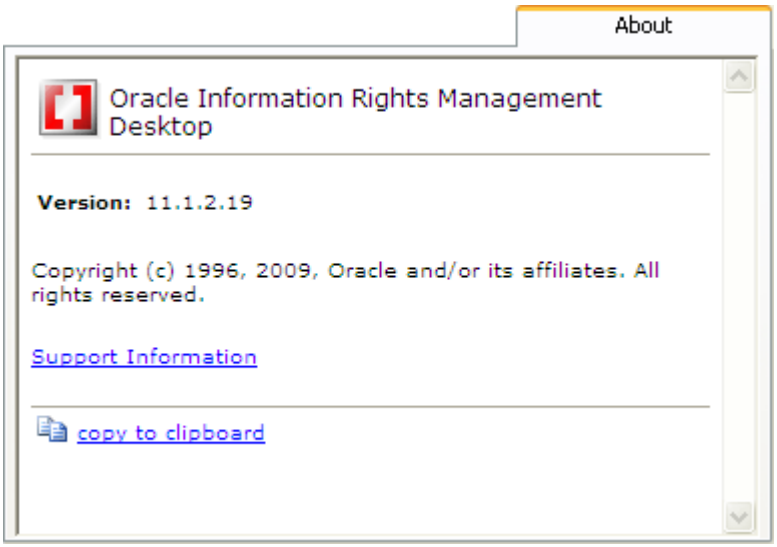
Item	Description
Enable sealed email integrations	Shows the supported mail clients and whether they are currently enabled for use with Oracle IRM Desktop. Mail clients not available on your computer are shown dimmed. Enabled mail clients are shown checked. To disable a mail client, uncheck it.
Settings (button)	Click to open the Sealed Email Options Dialog, through which you can: ▪ Specify a signature to include in sealed email, and whether to use it for new sealed email and/or replies to existing sealed email. ▪ Specify a template for sealed email. ▪ Specify text that will be placed in the body of an email to which sealed email is attached. ▪ Specify how you want sealed replies to appear. ▪ Specify whether you want your sealed email to be created in the default format (Microsoft Word), in plain text, or in rich text format.

A.1.7 About Tab

The About tab provides information about Oracle IRM Desktop, such as its version number and copyright information.

The tab also provides a Support Information link that you can use to collect information to assist support staff with problem diagnosis. If asked to provide further information about your Oracle IRM configuration, click the Support Information link and send the resultant file to your support representative.

Open the tab by selecting **About** on the Oracle IRM Desktop Options dialog. The About tab is also available from several other places, including the Oracle IRM Desktop Options dialog, the Oracle IRM Desktop Control Panel, and the Oracle IRM Desktop icon in the display notification area (system tray).

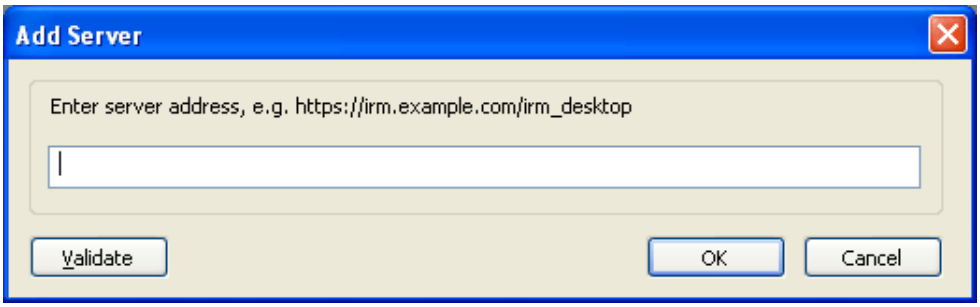


Element	Description
Information area	Information about Oracle IRM Desktop.
Support Information (link)	Opens the Oracle IRM Desktop Support Information Dialog, through which information can be collected that is useful to support staff.
Copy to clipboard (link)	Copies the version and copyright information to the clipboard, from where it can be pasted into a text application.

A.1.8 Add Server Dialog

Use the Add Server dialog to specify the URL of an Oracle IRM server.

Open the dialog by selecting the **New** or **Edit** buttons on the Servers tab of the Oracle IRM Options dialog, or on the Indexing Service Configuration dialog.



Item	Description
Input box	Enter the URL of an Oracle IRM server. For connection to an 11*g* server, the URL will be in the form `https://servername:port/irm_desktop` For connection to a 10*g* server, the URL will be in the form `seal://servername:80`

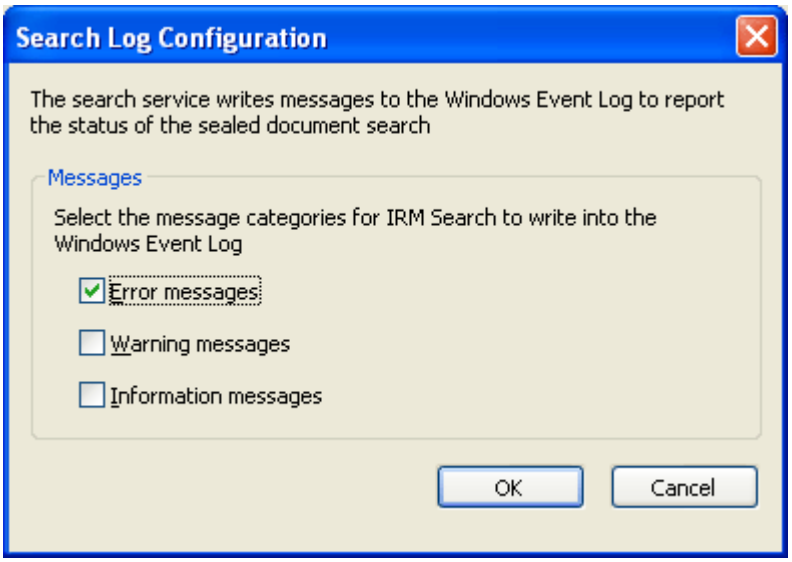
Item	Description
Validate (button)	Attempts to contact the server specified in the input box and validate the URL against the one configured on the Oracle IRM Server. This may not be the same URL entered here, and if successful the URL may be updated to match the one configured on the server. Success or failure is reported in a message dialog. If this option is not used, the URL is validated on clicking **OK**.

A.1.9 Search Log Configuration Dialog

The search service writes messages to the Windows event log to report the status of the sealed document search.

Use the Search Log Configuration dialog to select which search message types are written to the Windows event log.

Open the dialog by selecting the **Settings** button on the Search tab of the Oracle IRM Desktop Options dialog.



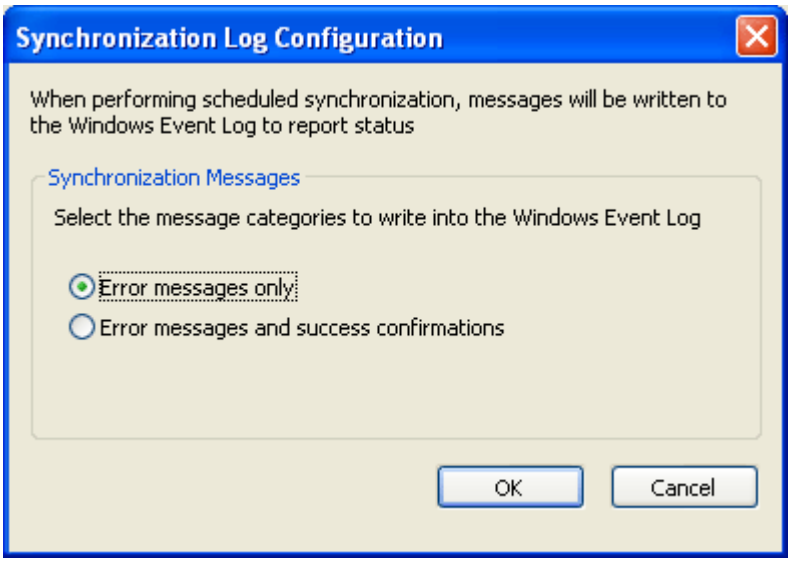
Item	Description
Messages	For each message type that you want to appear in the Windows event log, make sure that its checkbox is checked.

A.1.10 Synchronization Log Configuration Dialog

The synchronization manager writes messages to the Windows event log to report its status.

Use the Synchronization Log Configuration dialog to select which synchronization message categories are written to the Windows event log.

Open the dialog by selecting the **Log Settings** button on the Update Rights tab of the Oracle IRM Desktop Options dialog.



Item	Description
Synchronization Messages	Select either **Error messages only** or **Error messages and success confirmations**.

A.1.11 Indexing Service Configuration Dialog

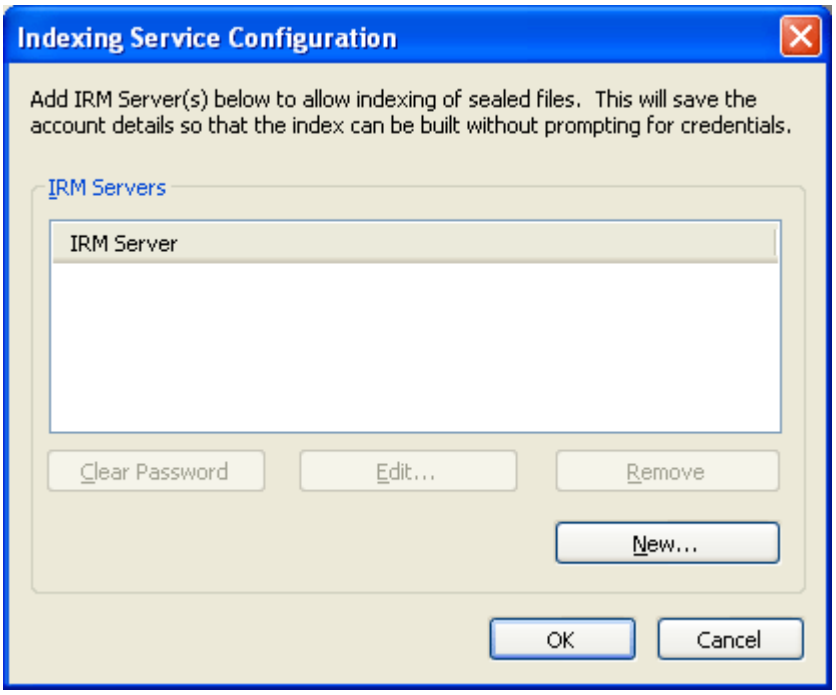
You can configure the Oracle IRM Desktop search feature to use the Microsoft indexing service to support sealed documents. Indexing makes searches more efficient, and is essential for searching within the Microsoft Windows 2008, Windows Vista, and Windows 7 operating systems.

The ability to create an index is subject to the rights of the account that the indexing service uses when requesting the right to search documents. This could be a user account, or could be an account created on the server specifically for the indexing service. For example, if you are setting up an index on a file server rather than an end user system, you might want the indexing service to have its own account on the server so that it can create indexes even if it is not running under a user account. You would need to consult the server administrator to arrange for an account and the associated Search right. See About Rights. The configuration is machine-wide, and only accounts using basic (username/password) authentication can be used as Search accounts.

When the indexing service tries to index sealed documents, it refers to the server for search rights. If successful, the sealed documents are indexed. Note that, if the indexed folders contain sealed documents that are authorized by different servers, you need to add each of the servers to the list in this dialog.

> **Note:** Search indexes created as described in this section are not restricted to the account holding the Search right: they can be read by anyone with access to the host computer.

Open the dialog by selecting the **Advanced** button on the Search tab of the Oracle IRM Desktop options dialog.



Item	Description
[Oracle] IRM Server (list area)	This list is initially empty. When populated, the list shows the URL, authentication type, and username of servers that manage the rights for the sealed documents that you want to be included in the search index. To add a server to the list, click the **New** button.
Clear Password (button)	For the highlighted server, clears the stored username and password entered from this instance of Oracle IRM Desktop. You will need to clear the password if you have more than one user identity on the server and you wish to change from one identity to another (perhaps because the different identities have different search and document access rights associated with them). When you select the Clear Password button, you see a message that tells you either that the stored password has been cleared, or that no passwords are stored for the server. After the password has been cleared, you will be prompted to supply a username and password the next time that you perform a search or index operation that involves a sealed document.
New (button)	Click to open the Oracle IRM Server URL dialog. Through this you can enter the URL of a server that controls the rights for the sealed documents that you want to be able to index.
Edit (button)	Applies to the server currently highlighted in the list. Click to reopen the Oracle IRM Server URL dialog, through which you can change the details for the server.
Remove (button)	Click to remove the currently highlighted server from the list.

A.2 Sealed Email Options Dialog

Open the dialog from the Email tab of the Oracle IRM Desktop Options dialog, by selecting at least one email client checkbox then selecting the **Settings** button.

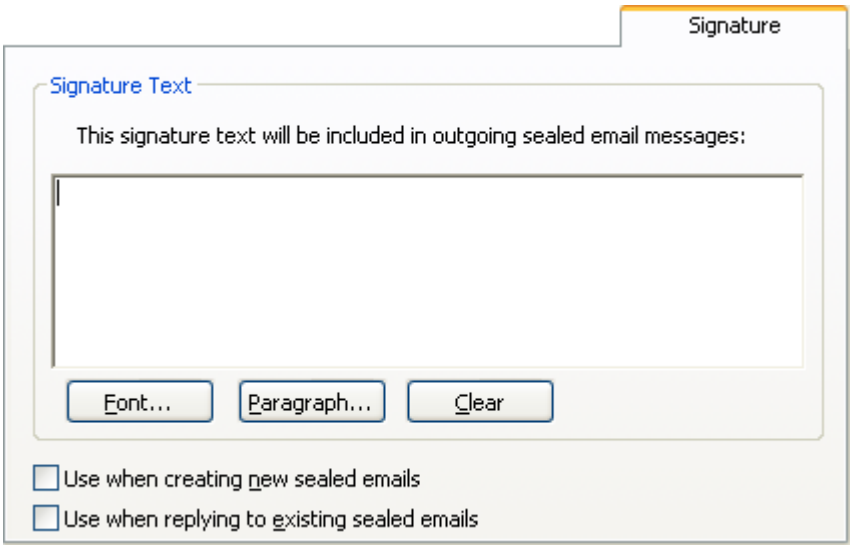
The following tabs are used to set options for sealed email in Oracle IRM Desktop:

- Signature Tab
- Email Template Tab
- Email Body Tab
- Sealed Reply Settings Tab
- Sealed Email Format Tab

A.2.1 Signature Tab

Use to specify signature text to include in sealed email, and whether to use it for new sealed email and/or replies to existing sealed email.

Open the tab by selecting **Signature** on the Sealed Email Options dialog.

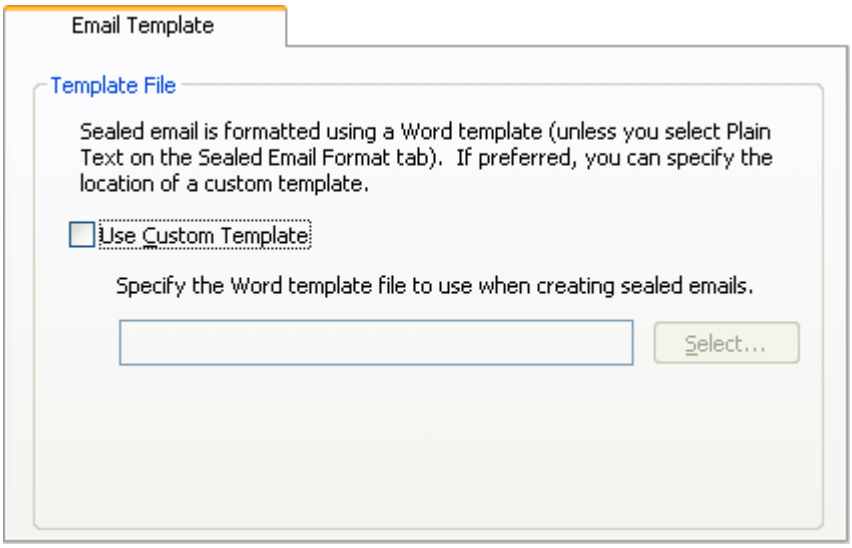


Item	Description
Signature Text	**Text box:** Enter the text that will be used as the signature text. **Font:** Applies to the highlighted text. Click to open the Font dialog, through which you can choose the font, style, size, effects, and script to be used for the signature text. **Paragraph:** Click to open the Paragraph dialog, through which you can choose the alignment of the current paragraph and whether it is bulleted. **Clear:** Click to clear the contents of the signature text box.
Use when creating new sealed emails (checkbox)	Normally unchecked. Check to use the signature when creating new sealed emails.
Use when replying to existing sealed emails (checkbox)	Normally unchecked. Check to use the signature when replying to existing sealed emails.

A.2.2 Email Template Tab

Use to specify a custom template for sealed email. A standard template is provided as part of the Oracle IRM Desktop installation. A custom template is a Microsoft Word template that you or your administrator provides. You can select a Microsoft Word template even if you use rich text format for sealed email. A custom template can include Oracle IRM fields or other visual reminders that the email contains sensitive information. Templates are not used if you select plain text format for sealed email.

Open the tab by selecting **Email Template** on the Sealed Email Options dialog.

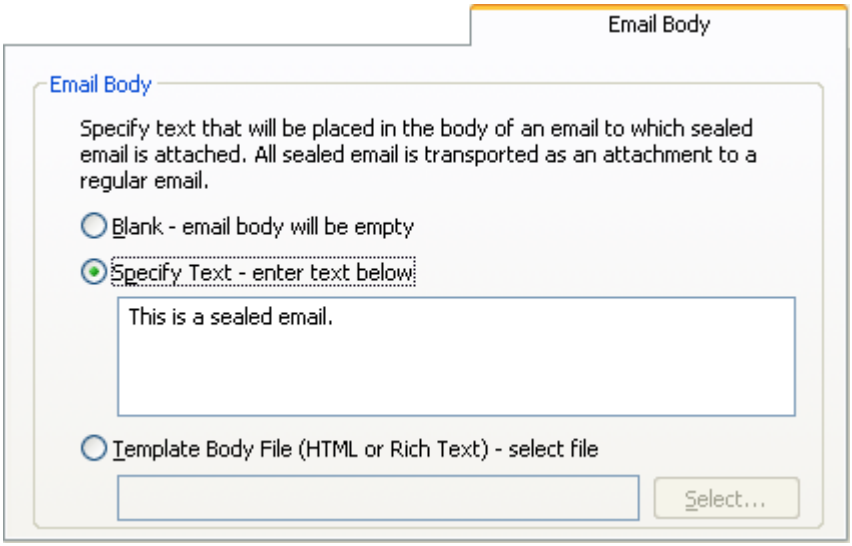


Item	Description
Template File	**Use Custom Template:** Normally unchecked. Check if you have a custom template that you want to use instead of the standard template. **Microsoft Word template file box:** This is available if you have checked the **Use Custom Template** box. Enter the location of the file that you want to use, or click the **Select** button to open a dialog through which you can find the required file.

A.2.3 Email Body Tab

Use to specify text that will be placed in the body of an email to which sealed email is attached. All sealed email is transported as an attachment to a regular email. You could, for example, specify some text to say `""Please see the sealed attachment."`

Open the tab by selecting **Email Body** on the Sealed Email Options dialog.

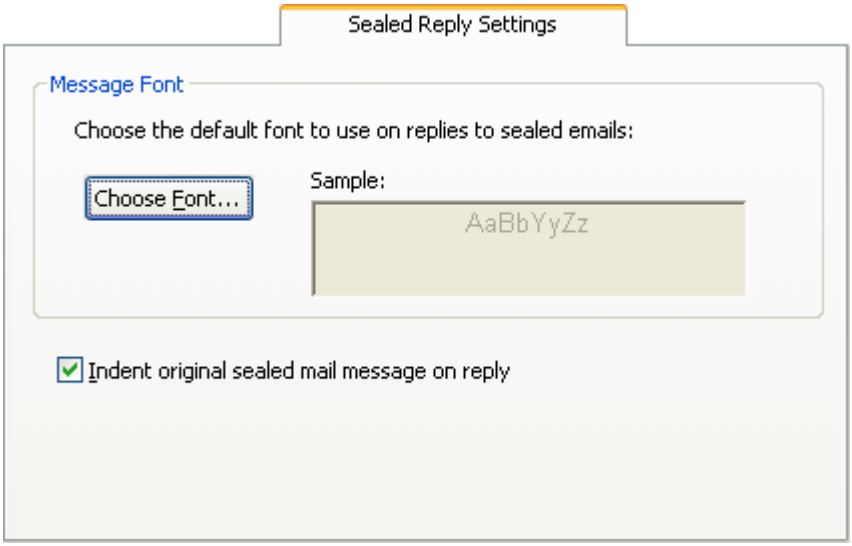


Item	Description
Email Body	**Blank:** Select if you want the body of the accompanying unsealed email to be blank. **Specify Text:** Normally selected. If selected, the accompanying text box is available for entering the text that you want in the email body. The default text is "This is a sealed email.". Overtype the current text with text of your own. **Template Body File:** Select if you want to use text in an HTML or rich text format file in the body of the email. If selected, the accompanying entry box is available. Enter the location of the file that you want to use, or click the **Select** button to open a dialog through which you can find the required file.

A.2.4 Sealed Reply Settings Tab

Use to specify how you want sealed replies to appear.

Open the tab by selecting **Sealed Reply Settings** on the Sealed Email Options dialog.

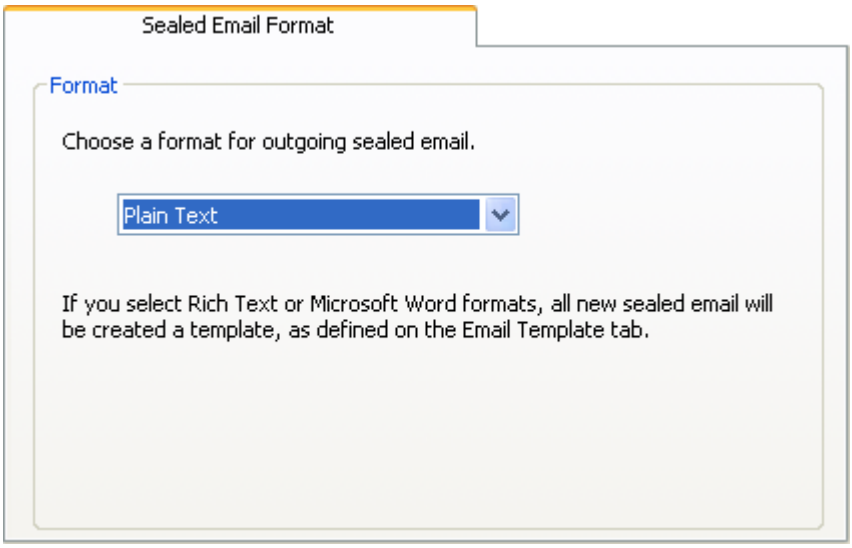


Item	Description
Message Font	**Choose Font:** Click to open the font dialog, through which you can select the font, style, size, effects, and script for the text in replies to sealed emails. The font options that you choose are applied to the text in the Sample box.
Indent original sealed mail message on reply (checkbox)	Normally checked.

A.2.5 Sealed Email Format Tab

By default, your sealed email will be created in Microsoft Word format. If you prefer, you can specify that you want sealed email to be in plain text or rich text format. We recommend that you use the default format, although the other formats produce smaller email attachments. Using Microsoft Word format ensures backwards compatibility with previous versions of the Oracle IRM software, and provides better edit options, particularly for users whose rights require all changes to email to be tracked. The format you select for sealed email has no influence on the format of any sealed documents you attach to your sealed email.

Open the tab by selecting **Sealed Email Format** on the Sealed Email Options dialog.



Item	Description
Format	Normally set to Microsoft Word. Select a format from the drop-down list.

A.3 Oracle IRM Desktop Control Panel Dialog

The Oracle IRM Desktop Control Panel dialog provides access to a set of tabs that show information about the specific sealed document you are currently viewing, including your rights within the sealed document. It is accessed from the Oracle IRM icon in the toolbar of a sealed document, or by selecting the **Control Panel** link on any status page.

The Oracle IRM Desktop Control Panel dialog can display the following tabs, depending on what type of sealed document you currently have open:

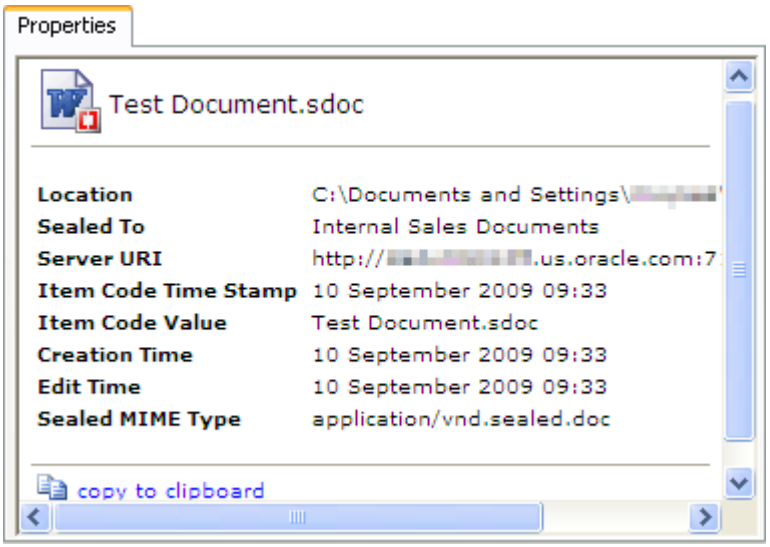
- Properties Tab
- Rights Tab
- About Tab
- Account Tab

A.3.1 Properties Tab

The Properties tab shows the properties of the sealed document you are currently viewing, such as when it was sealed and to which context.

The properties can help with diagnostics.

Open the tab by selecting **Properties** on the Oracle IRM Desktop Control Panel dialog, which you open by selecting the **Oracle IRM** icon in the toolbar of a sealed document, or by selecting the **Control Panel** link on any status page.



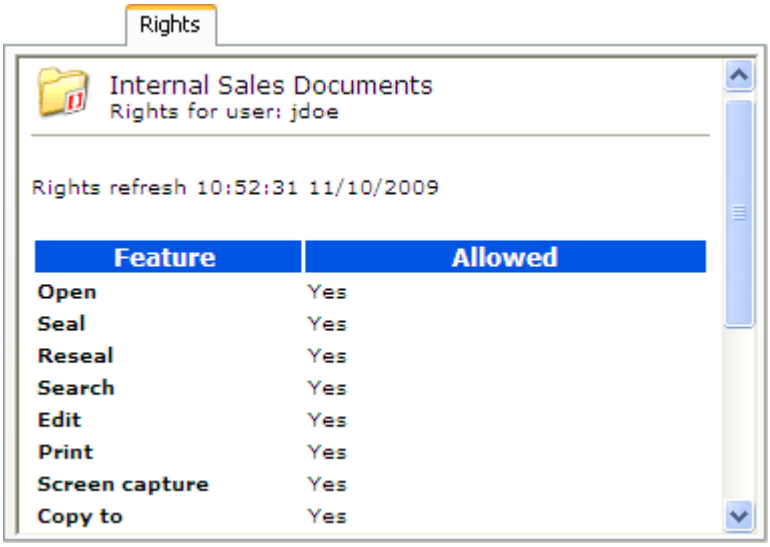
Element	Description
Scrollable display area	Shows the properties of the sealed document you are currently viewing.
Copy to clipboard (link)	Copies the properties information to the clipboard, from where it can be pasted into a text application.

A.3.2 Rights Tab

The Rights tab shows what rights you have for the current document, and when these rights have to be refreshed.

The list can vary depending on the type of sealed document you are viewing. For example, rights related to playing video files only appear when you access a video file.

Open the tab by selecting **Rights** on the Oracle IRM Desktop Control Panel dialog, which you open by selecting the **Oracle IRM** icon in the toolbar of a sealed document.

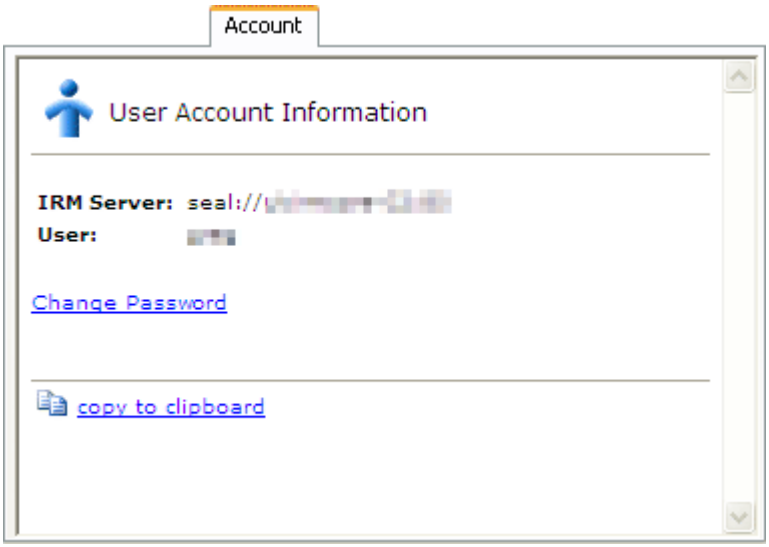


Element	Description
Document information display area	Shows, in the following order: ■ the name of the context to which the current document is sealed ■ the name of the document user ■ the time and date by which the rights held for the current document have to be refreshed (by synchronization with the server).
Feature (column)	Features equate to rights. The Features column lists the rights that have been allocated to the current user for the current sealed document. Not all rights are listed. Where a main right includes a subsidiary right, and where both rights have been allocated to the current user, only the main right is shown. The following are examples of such compound rights: ■ The Edit right includes the Edit Tracked, Annotate, Interact, and Formulae rights. ■ The Print to File right includes the Print right. If you have been allocated a subsidiary right, but not the main right, both rights are shown in the Features column, the subsidiary right with "Yes" against it, and the main right with "No" against it.
Allowed (column)	""Yes" shows that the right has been allocated to the current user for the current sealed document. "No" shows that the right has not been so allocated.
Trusted Destinations (display area)	You may have to scroll down to see this. If you have the Copy To right, a list of trusted destinations that you can reseal to and copy text to is shown here. Note that if you have the Copy right, you will not have the Copy To right. This is because you do not need the Copy To right if you have the Copy right: with the Copy right, you can copy material from sealed documents to any other document, whether or not it is in a trusted destination.
Copy to clipboard (link)	You may have to scroll down to see this. Select to copy the rights information to the clipboard, from where it can be pasted into a text application.

A.3.3 Account Tab

The Account tab identifies the server and user for a document sealed against a 10*g* version of Oracle IRM Server. The tab is shown only for documents sealed against a 10*g* version of Oracle IRM Server.

Open the tab by selecting **Account** on the Oracle IRM Desktop Control Panel dialog, which you open by selecting the **Oracle IRM** icon in the toolbar of a sealed document.



Element	Description
Oracle IRM Server	Shows the 10*g* server against which the current document was sealed.
User	Shows the username for the current user of the sealed document.
Change Password (link)	Opens the Change Password Dialog (10g only), through which you can change the current user's password for accessing sealed documents on the current server. You will need to enter the old password before you are allowed to create a new password. This method of changing a password applies only to 10*g* servers.
Copy to clipboard (link)	Copies the user account information to the clipboard, from where it can be pasted into a text application.

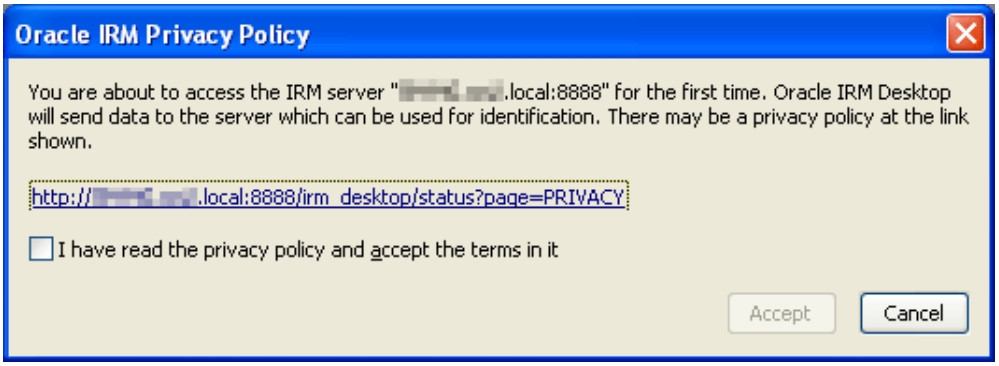
A.4 General Features

This section describes the dialogs that are available from various parts of the product. These include:

- Oracle IRM Privacy Policy Dialog
- Select Context Dialog
- Change Item Code Dialog
- Status Page Dialog
- File Report Dialog
- Sealed File Properties (Oracle IRM) Tab
- Oracle IRM Server Connection Test Dialog
- Oracle IRM Desktop Support Information Dialog
- Change Password Dialog (10g only)
- Protected View Message Dialog

A.4.1 Oracle IRM Privacy Policy Dialog

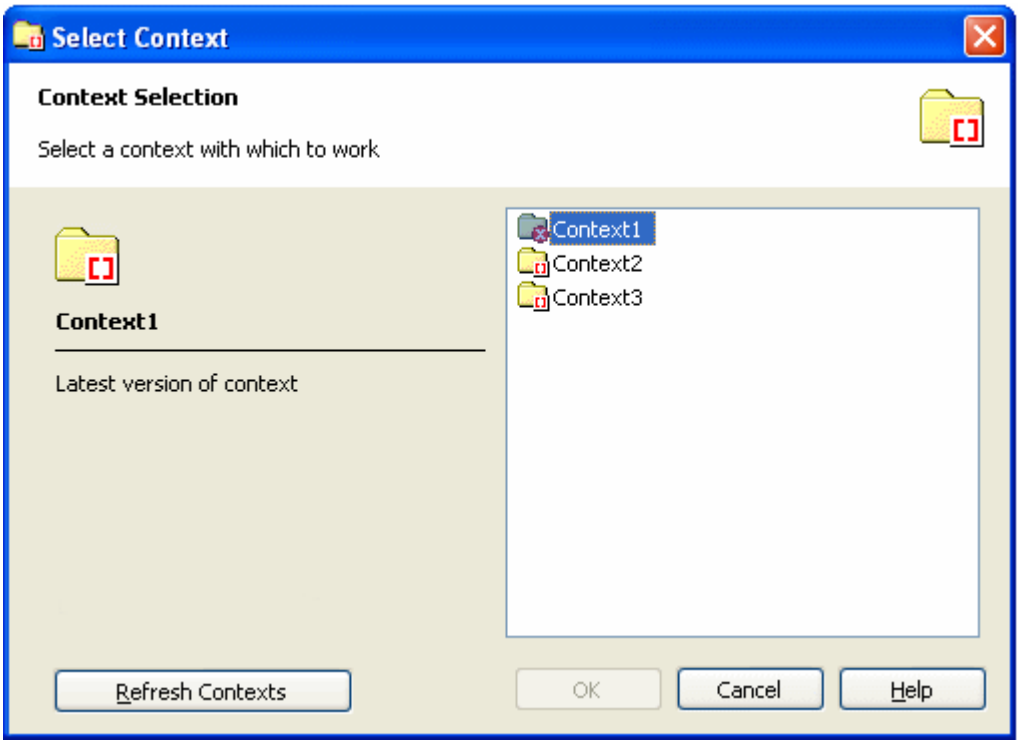
This dialog will be displayed when you attempt to connect to an Oracle IRM Server for the first time.



Element	Description
Link	This may link to the privacy policy that applies to the use of the sealed document that is about to be opened. The policy and its accessibility from this link is controlled by the owner of the Oracle IRM Server instance.
I have read... (checkbox)	Initially unchecked. Check if you agree with the statement. If you do not agree, you will not be able to see the sealed document. To proceed, you must check the box even if the server owner has not provided a privacy policy.
Accept (button)	This becomes available if the "I have read..." box is checked. Select to open the sealed document.

A.4.2 Select Context Dialog

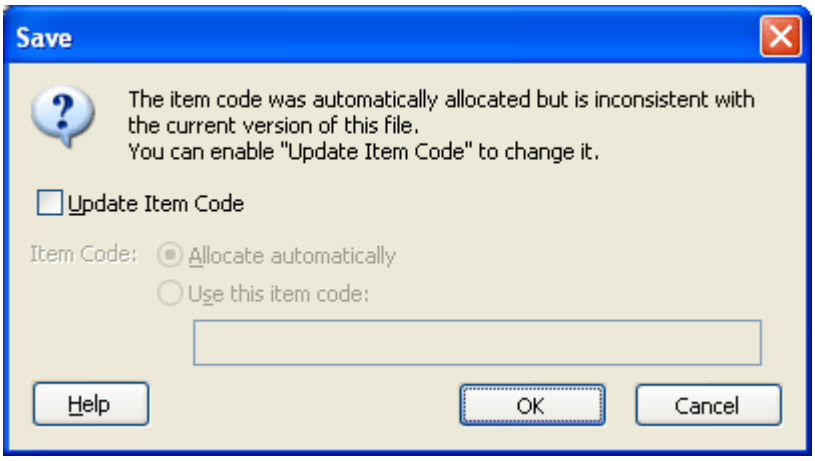
For tasks that involve sealing or resealing documents, you will be prompted to select a context for that operation. In all cases, you will see the same context selection dialog.



Element	Description
Context Selection information area and list box	Lists the contexts that you have the right to seal or reseal to. Usually provides a description of each context to help you choose the right one for the document or email you are currently sealing. If the list is blank and you are trying to create a new sealed document, you must first connect to a server that holds context definitions that you have been given permissions to use. The easiest way to set up such a connection is to open a document that has been created by someone else and sealed to the same server and context to which you want to seal your new document. If this is not possible, you can connect to a server through the Servers tab on the Oracle IRM Desktop Options dialog. Do do this, you will need to know the URL of the server that you want to connect to. This will be in the following form: `https://servername:port/irm_desktop` You can obtain the exact URL from the administrator of the server.
Refresh Contexts (button)	Use to update the list of contexts, if you think it is incomplete. The list can be incomplete if your rights have changed recently such that your local cache is out of date.

A.4.3 Change Item Code Dialog

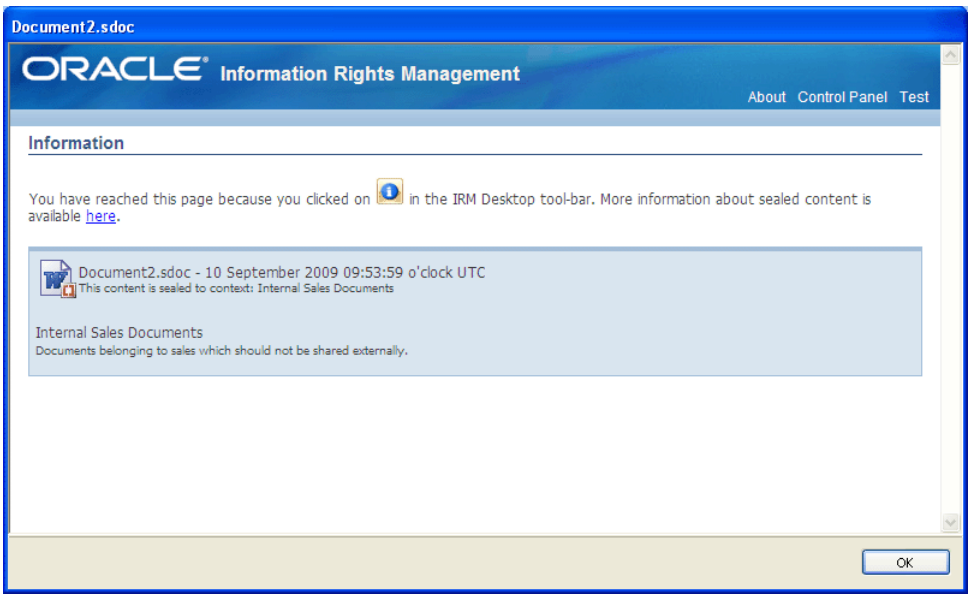
This dialog will be displayed if you try to save a sealed document with an out of date item code and you have the right to update the item code (Set Item Code right). This may happen when you rename a sealed document, then edit it and save it.



Element	Description
Update Item Code (checkbox)	Normally unchecked. Check if you want to update the out of date item code.
Item Code	**Allocate automatically:** Select to have a new item code generated by Oracle IRM Desktop. **Use this item code:** Select if you already have an item code that you want to allocate to this document. Selecting this option activates the accompanying input box, into which you can enter the new item code.

A.4.4 Status Page Dialog

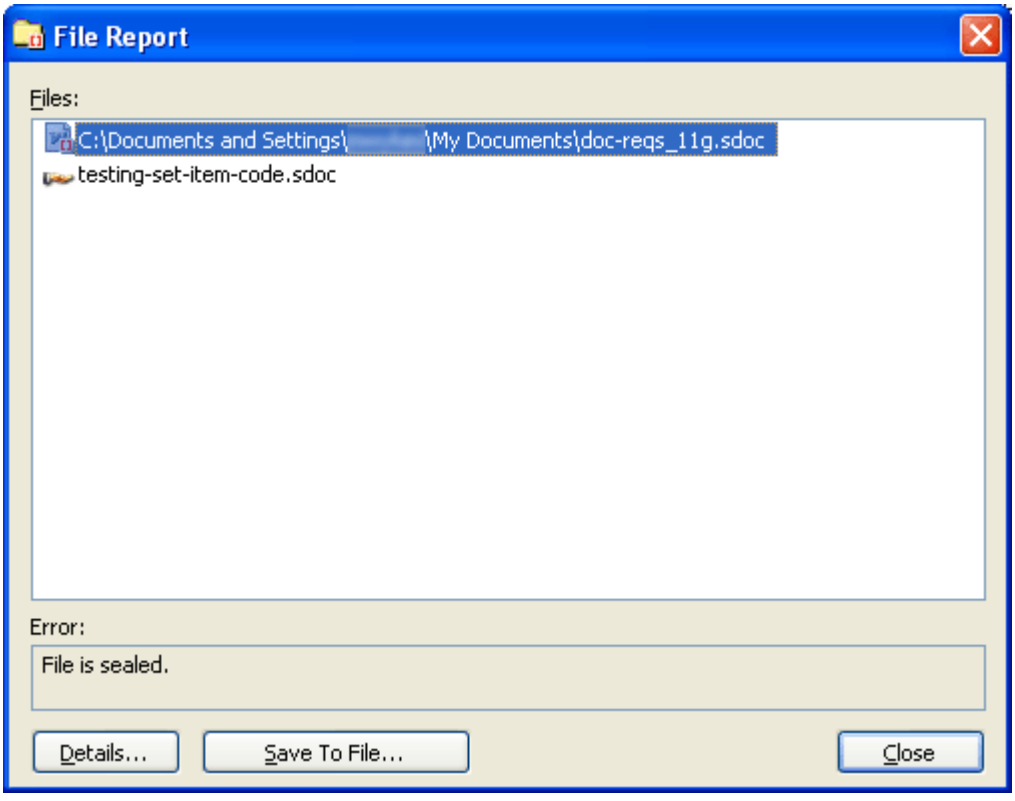
Open this dialog by selecting the **Online Information** icon on the Oracle IRM toolbar in a sealed document. This dialog opens automatically if sealed content cannot be displayed because of a problem.



Element	Description
Information area	Gives the reasons why this dialog has opened. **Rights held on another computer:** This usually means that the sealed document cannot be viewed on the current computer until the rights have been checked in on another computer. Click **Which Computer** to identify the other computer. If the computer is identified as the one you are currently at, it is probable that the device ID has been changed since the rights information was initially requested: in this case, ask the server administrator to check in or reset the rights on the server.
About (link)	Links to a source of more information about Oracle IRM sealed content.
Control Panel (link)	Opens the Oracle IRM Desktop Control Panel.
Test (link)	Opens the Oracle IRM Server Connection Test Dialog, through which you can test your connection to servers.
Help (link)	Opens the Oracle IRM Desktop online help system.

A.4.5 File Report Dialog

This dialog shows the results of a sealing operation when one or more files failed to seal.

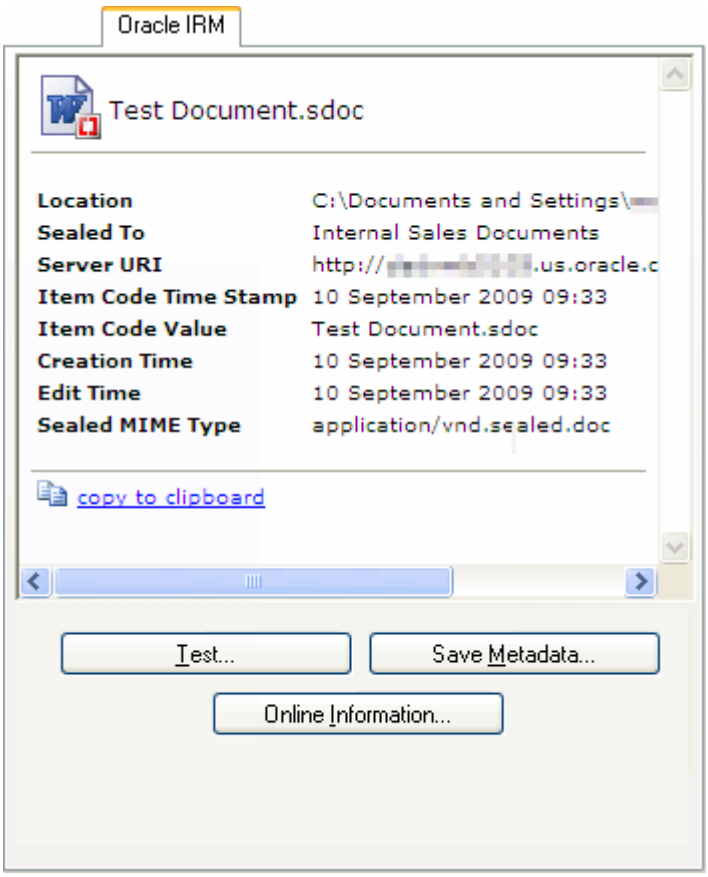


Element	Description
Files (list)	Lists the files that were not sealed during the recent sealing operation.
Error (display)	Shows the error related to the highlighted item in the Files list. Gives the reason why a file was not sealed.

Element	Description
Details (button)	Opens a dialog showing more details, if available, about why the file was not sealed.
Save to File (button)	Opens the Save As dialog to let you save the details in this report dialog as a text file.

A.4.6 Sealed File Properties (Oracle IRM) Tab

Open the tab by right-clicking the filename of a sealed document in a file browser and selecting **Properties**, then selecting the **Oracle IRM** tab.

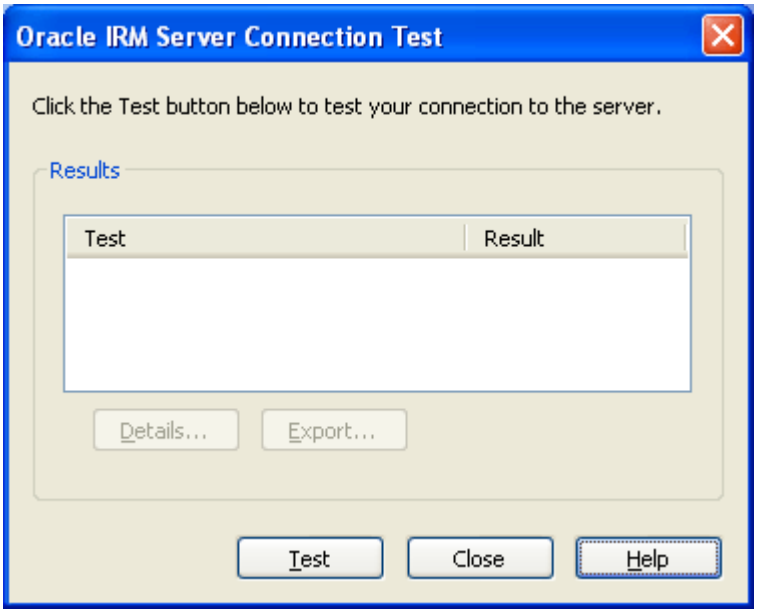


Element	Description
Scrollable display area	Shows the properties of the document you are currently viewing.
Copy to clipboard (link)	Copies the properties information to the clipboard, from where it can be pasted into a text application.
Test (button)	Opens the Oracle IRM Server Connection Test Dialog, through which you can test your connection to servers.
Save Metadata (button)	Enables you to save a copy of the sealed file metadata in XML format.
Online Information (button)	Use this button to go to a web page where the content originator will provide more information about your account, your rights, and the current content.

A.4.7 Oracle IRM Server Connection Test Dialog

This dialog is available from Oracle IRM Desktop status pages, and from the **Test** button on the Oracle IRM tab in the properties dialogs for sealed documents.

The Server Connection Test dialog can help to diagnose network problems and help your administrator to resolve them.

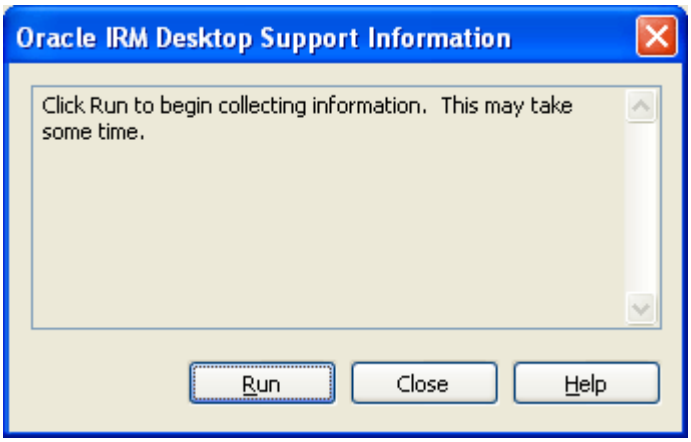


Element	Description
Results	**Test column:** Identifies each test. Usually includes a simple connection test to the server, which requires no authentication of the user. Also usually includes an authenticated connection to the server, for which user credentials may have to be supplied through the Oracle IRM Server Credentials dialog. **Result column:** Shows the result of the test (Pass, Fail, Canceled). **Details button:** Select to open a message box with more information about the tests, if there is any. **Export button:** Select to open a dialog through which you can save the test information as an HTML document.
Test (button)	Starts the test routine.

A.4.8 Oracle IRM Desktop Support Information Dialog

This dialog is available from the Support Information link on About tabs.

Use this dialog to create a text file containing information about your installation and environment.

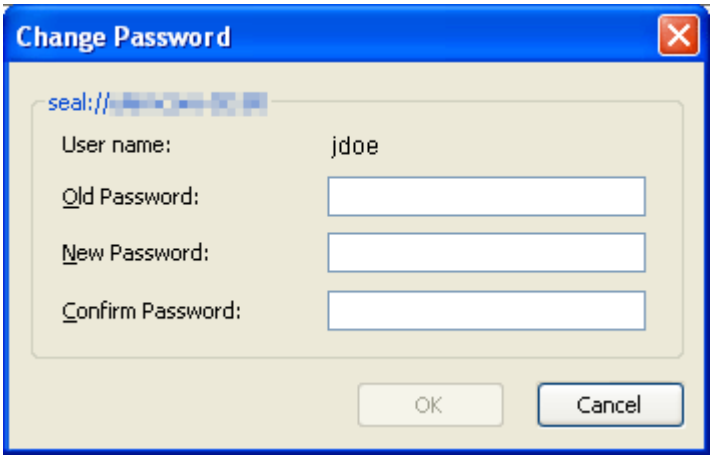


Element	Description
Information display area	Initially contains advice and instructions. When the **Run** button is selected, this area shows the progress, and then gives the names and location of the text files containing the gathered support information.
Run (button)	Starts the gathering of support information.

A.4.9 Change Password Dialog (10*g* only)

This dialog is available from the Change Password link on the Account tab of the Oracle IRM Desktop Control Panel. The Account tab is available only for some documents sealed against a 10*g* server.

Use this dialog to change the password used by the current user to access documents sealed on a 10*g* server.

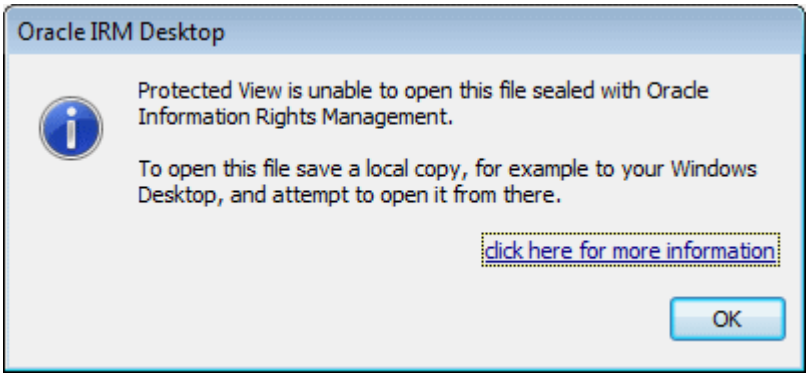


Element	Description
Server name (display)	Shows the name of the server on which the current document is sealed, and for which the password change will apply.
User name (display)	Shows the name of the current user.
Old Password (text box)	Enter the current password for the user shown above.
New Password (text box)	Enter the new password to be used for the user shown above.

Element	Description
Confirm Password (text box)	Enter the new password again, in exactly the same way.

A.4.10 Protected View Message Dialog

This dialog is shown if you attempt to open a sealed Microsoft Office file from within a Microsoft Office application that has Protected View turned on. (Protected View is a Microsoft Office 2010 feature.)



The use of sealed documents when Protected View is turned on is described in the following topics:

- Section 4.1.2, "Opening a Sealed Document in a File Browser"
- Section 5.2, "Opening Sealed Email Messages and Sealed Attachments"

A.5 Oracle IRM Desktop Toolbars

This section describes the toolbars that are available when using sealed documents:

- Oracle IRM Desktop Toolbar in Internet Explorer
- Oracle IRM Desktop Toolbar in Microsoft Office
- Oracle IRM Desktop Toolbar in Microsoft Office 2007 and Microsoft Office 2010

The location and appearance of the Oracle IRM Desktop toolbar differs slightly depending on whether you are viewing sealed documents in Internet Explorer or in Microsoft Office applications:

- In Internet Explorer, when you are viewing sealed documents such as HTML and PDF, the Oracle IRM Desktop toolbar is shown at the top of the browser area.
- In Microsoft Office applications, the Oracle IRM Desktop toolbar is shown in the toolbar area.
- In Microsoft Office 2007 applications, the Oracle IRM Desktop toolbar is shown as a ribbon in the ribbons area.

A.5.1 Oracle IRM Desktop Toolbar in Internet Explorer

The toolbar contains the following buttons, from left to right:

Button	Definition
Control Panel	Used to open the Oracle IRM Desktop Control Panel.
Save	Use this button to save changes to sealed documents while you are working on them, if you have the right to reseal.
Print	Use this button to print sealed content, if you have the right to print.
Synchronization and Check In	Use to open the the Update Rights Tab on the Oracle IRM Desktop Options dialog. You can use this tab to update your rights from Oracle IRM Server, or to check in your rights so that they can be used from another device.
Online Information	Use this button to go to a web page where the content originator will provide more information about your account, your rights, and the current content.

A.5.2 Oracle IRM Desktop Toolbar in Microsoft Office

The toolbar contains the following buttons, from left to right:

Button	Definition
Control Panel	Used to open the Oracle IRM Desktop Control Panel.
Synchronization and Check In	Use to open the the Update Rights Tab on the Oracle IRM Desktop Options dialog. You can use this tab to update your rights from Oracle IRM Server, or to check in your rights so that they can be used from another device.
New Sealed	Use this button to create a new sealed document or a new sealed document from a sealed template.
Open Sealed	Use this button to open a dialog through which you can open existing sealed documents.
Save as Sealed	Use this button to create a sealed version of the current unsealed document.
Online Information	Use this button to go to a web page where the content originator will provide more information about your account, your rights, and the current content.

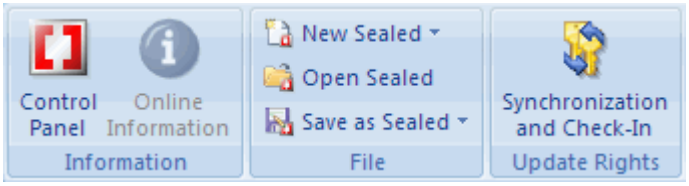
You can drag the Oracle IRM Desktop toolbar to a different location within the toolbar area, just as for any other toolbar in Microsoft Office.

Beneath the toolbar area in Microsoft Office is the Oracle IRM information bar (if the option to display it has been selected in the Oracle IRM Desktop Options dialog).

The information bar usually shows which context the document is sealed to.

A.5.3 Oracle IRM Desktop Toolbar in Microsoft Office 2007 and Microsoft Office 2010

The toolbar contains the following buttons:



Button	Definition
Control Panel	Used to open the Oracle IRM Desktop Control Panel.
Online Information	Use this button to go to a web page where the content originator will provide more information about your account, your rights, and the current content.
New Sealed	Use this button to create a new sealed document or a new sealed document from a sealed template.
Open Sealed	Use this button to open a dialog through which you can open existing sealed documents.
Save as Sealed	Use this button to create a sealed version of the current unsealed document.
Synchronization and Check In	Use to open the the Update Rights Tab on the Oracle IRM Desktop Options dialog. You can use this tab to update your rights from Oracle IRM Server, or to check in your rights so that they can be used from another device.

Index

A

account lock-out, 9-4
authentication settings, 2-8

C

capturing images, 4-12
checking in rights, 7-3
clipboard, 4-3
connecting
  to Oracle IRM Server, 7-2
connection
  to Oracle IRM Server, 1-6
contexts, 1-5
  changing, 4-7
creating sealed documents, 4-4, 4-6
  using Microsoft Office, 4-5
  using Windows Explorer, 4-4

D

desktop sealing settings, 2-4
document extensions, 9-6
document formats, 9-6
documents
  adding Oracle IRM fields, 6-1
  opening, 3-1
  sealing, 3-2

E

editing sealed documents, 4-3
  using clipboard, 4-3
email
  creating sealed, 5-2
  creating sealed replies, 5-4
  forwarding, 5-5, 5-6
  forwarding with amendment, 5-6
  forwarding without amendment, 5-5
  integrated email applications, 5-2
  opening sealed, 5-3
  replying, 5-4
  replying to sealed, 5-5
  sealed, 1-7, 5-1
  sealing, 5-6
  sending sealed, 5-2
  using existing attachments, 5-2
  using sealed email document format, 5-2
email settings, 2-7
embedded objects, 9-4
extensions, 9-6
extracting MSI file, 2-9

F

fields, 1-8
  adding in Microsoft Excel, 6-3
  adding to document, 6-1
  adding to Microsoft Word, 6-1
  list of, 9-1
  registering as Microsoft Word document properties, 6-2
  using with Microsoft Word, 6-3
file icons, 9-6
firewalls, 9-5
formats, 9-6
forwarding email, 5-5, 5-6

G

getting started, 3-1

I

icons, 9-6
installation, 2-1
  procedure, 2-1
  silent, 2-3
  unattended, 2-3
  uninstalling, 2-2
integrating Lotus Notes, 2-10
item codes, 1-6

L

legacy setting, 2-8
local data clean-up setting, 2-8
lock-out, 9-4
log files
  search, 4-10
Lotus Notes
  integration, 2-10

M

Microsoft Excel, 4-12
  adding Oracle IRM Fields, 6-3
  linking spreadsheets, 4-13
  updating links, 4-13
Microsoft Indexing Service, 4-10
Microsoft Office, 4-2, 4-5
  enabling integration, 3-4
  SharePoint behavior, 8-1
  templates, 4-14
Microsoft Word
  adding Oracle IRM fields, 6-1
  registering Oracle IRM fields, 6-2
  using Oracle IRM fields, 6-3
MIME types, 9-6
MSI file
  extracting, 2-9
multimedia files, 1-7

O

opening sealed documents, 3-1, 4-1
  in Microsoft Office, 4-2
  in Windows Explorer, 4-1
opening sealed email, 5-3
operating systems, 2-1
Oracle IRM
  about, 1-1
Oracle IRM fields, 1-8
  list of, 9-1
Oracle IRM Server
  connecting manually, 7-2
  connecting to, 1-6
  synchronizing with, 1-6

P

printing sealed documents, 4-10
Protected View, 4-2, 5-3, 5-4
proxy servers, 9-5

R

Registry key information, 9-9
Registry key policy setting, 2-10
replying to email, 5-4
rights, 1-2
  checking in, 7-3
  managing, 7-1
  obtaining, 7-1
  on shared computers, 7-2
  synchronizing manually, 7-3

S

saving changes, 4-6
screen captures, 9-6
screen capturing, 4-11
sealed documents, 1-2
  capturing image from, 4-12
  changing context, 4-7
  creating, 4-4
    from unsealed document, 4-6
  creating new, 3-3
  editing, 4-3
  item codes, 1-6
  opening, 3-1, 4-1, 4-2
  Oracle IRM fields, 1-8
  printing, 4-10
  saving changes, 4-6
  screen capturing, 4-11
  searching, 4-8
  unsealing, 4-8
  watermarks, 1-8
  working with, 4-1
sealed email, 1-7, 5-1
sealed multimedia files, 1-7
sealed presentations, 4-11
sealing
  existing document, 3-2
search logging, 4-10
search settings, 2-6
searching sealed documents, 4-8
  configuring logging, 4-10
  enabling search, 4-9
  Microsoft Indexing Service, 4-10
sending email, 5-6
settings
  authentication, 2-8
  desktop sealing, 2-4
  email, 2-7
  legacy, 2-8
  search, 2-6
  synchronization manager, 2-5
shared computers, 7-2
SharePoint, 8-1
sharing sealed presentations, 4-11
silent installation, 2-3
spreadsheets, 4-12
synchronization
  rights, 7-3
  with Oralce IRM Server, 1-6
synchronization manager settings, 2-5
system requirements, 2-1

T

templates
  creating sealed, 4-14, 4-15
  editing, 4-15
  Microsoft Office, 4-14

U

unattended installation, 2-3
uninstalling Oracle IRM Desktop, 2-2
unsealing, 4-8

V

VB code, 9-4

W

watermarks, 1-8, 9-4
web conferences, 4-11
Windows Explorer, 4-1, 4-4
working offline, 7-1