

Oracle Information Rights Management 10gR3 Quick Evaluation Guide

This document provides an overview of Oracle Information Rights Management. It enables you to perform an interactive evaluation of the end-user experiences of reading, creating and editing sealed documents and emails. This document is not intended to be a complete installation, administration or development guide, but rather a tutorial providing a rapid overview of the basic principles.

You will be invited to apply for an evaluation user account, which will enable you to experience many of the benefits of information rights management without needing to install any server software. Your account will be created on a hosted Oracle IRM Server, enabling you to quickly evaluate the technology.

Oracle Information Rights Management was previously known as SealedMedia E-DRM.

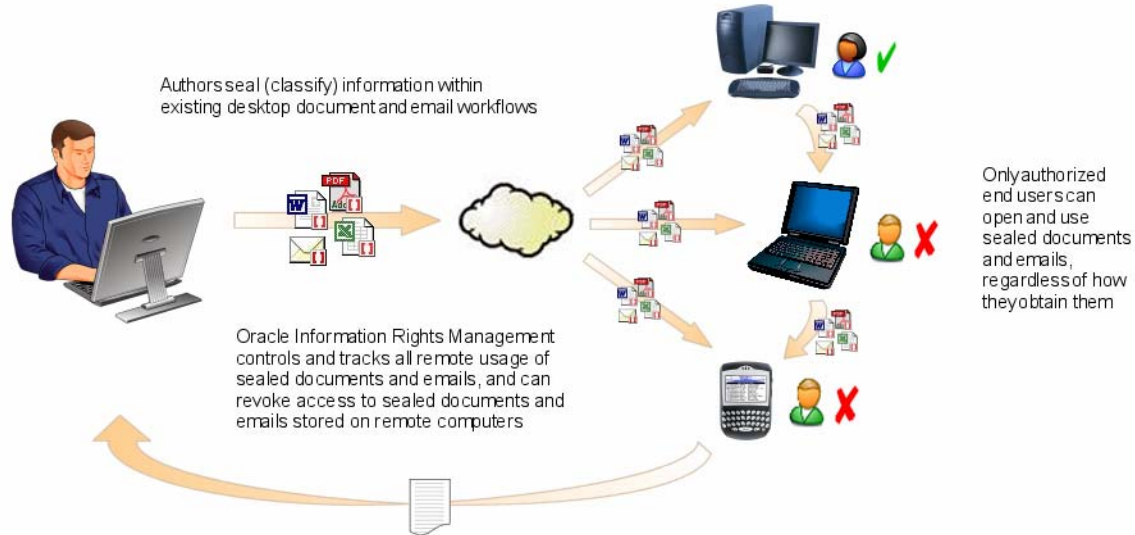
Contents

PRODUCT OVERVIEW	3
EVALUATION PROCESS	5
CREATING AN EVALUATION ACCOUNT	6
OPENING SEALED DOCUMENTS	7
ENABLING OFFICE INTEGRATION	8
SEALING DOCUMENTS	9
USING SEALED EMAIL	12
ACCOUNTS ON MULTIPLE SERVERS	17
SUMMARY	18

Product Overview

HOW ORACLE INFORMATION RIGHTS MANAGEMENT WORKS

Oracle Information Rights Management is a new type of information security solution, which uses encryption to “seal” documents and emails, and then carefully controls access to the decryption keys so that only authorized end users can open and use sealed documents and emails, regardless of where they are stored and used.



Unlike previous encryption solutions Oracle Information Rights Management enables authorized users to create and use sealed documents and emails transparently within existing desktop applications, such as Microsoft Office, Adobe Reader and Lotus Notes, without requiring any understanding or management of keys or passwords. A one-time install of the Oracle IRM Desktop supports current and previous versions of all standard desktop document and email applications, and continues to protect and track sealed documents and emails even while they are in use within those applications.

Unlike previous gateway and desktop monitoring solutions Oracle Information Rights Management also continues to protect and track sealed documents and emails when they are stored and used on desktops outside the firewall - for example within partners, suppliers, and outsourced or offshore facilities.

KEY BENEFITS

- Protect sensitive documents and emails from accidental or deliberate abuse, regardless of where they are stored, transmitted and used.
- Revoke access to sensitive documents and emails stored on remote desktops, when projects end, or employees/contractors leave.
- Enable controlled sharing of sensitive documents and emails across the heterogeneous desktop environments of real-world extended enterprises, without requiring end users to upgrade or change from existing desktop applications.

- Easily deploy to internal and external users, who can begin creating or using sealed documents and emails within minutes.
- Encourage adoption by being transparent to end users and minimizing impact to their existing document and email workflows.
- Offline creation and use of sealed documents and emails, without requiring any manual intervention by mobile end users.
- Supports and enforces clear and communicable information classification policies, based on existing business processes and employee roles.
- Opens an unprecedented window onto the actual use (or attempted abuse) of information on remote desktops inside and outside the firewall.
- Business process owners can now easily manage the security of their most sensitive information, without imposing undue load on IT administrators (or giving them blanket access).

PRODUCT COMPONENTS

- **Oracle IRM Desktop**
This enables authorized users to create and use sealed information, subject to rights obtained from the Oracle IRM Server. This product component is downloaded and used as part of this evaluation exercise.
- **Oracle IRM Server**
This stores the decryption keys and rights governing end user access to sealed documents and emails.
- **Oracle IRM Management Console**
This enables administrators to manage every aspect of the Oracle Information Rights Management solution.
- **Oracle IRM Standard Rights Model**
This web application enabling business and IT administrators to create new users, assign roles, etc.

Evaluation Process

Following the simple steps below will give you an excellent first hand experience of Oracle Information Rights Management from an end-user's perspective.

- Email irm_evaluation_request_ww@oracle.com stating your full name, company name and email address, to request an account to be created for you.
- You will receive an emailed response within 48 hours, giving you a username and password and a link to download the Desktop agent. The software can also be downloaded directly from <http://smweb.evaluation.sealedmedia.com>.
- After installing the Oracle IRM Desktop software, log in with your username and password and visit our [test page](#). If you see a picture of a fish everything is working correctly. You can check the Login automatically box, so that you do not need to login each time you unseal or seal a document.
- You will also receive a second email with three attachments. Try to open each of these documents and experience the different behavior depending on their level of required security.

In addition to this basic evaluation you can perform additional tasks to gain further familiarity with Oracle Information Rights Management.

- You can enable the Oracle IRM Desktop integrations with Office, Outlook and Notes email ... to give you sealing capabilities within Office and email applications, for simplified workflow.
- You can seal your own documents.
- You can send sealed emails (as well as sealed document attachments).
- If you ask your colleagues to request evaluation accounts, you can then share your own sealed documents and emails, gaining an enhanced appreciation of the evaluation.

Creating an Evaluation Account

REQUEST A USERNAME AND PASSWORD

Email irm_evaluation_request_ww@oracle.com stating your full name, company name and email address, to request an account to be created for you.

DOWNLOAD THE DESKTOP

You will receive an emailed response within 48 hours, giving you a username and password and a link to download the Desktop agent. This can also be downloaded directly from <http://smweb.evaluation.sealedmedia.com>

You should install the Oracle IRM Desktop software. After you have installed it, and logged in with your username and password, please visit our test page http://download.sealedmedia.com/unsealer/test_content.asp. If you see a picture of a fish everything is working correctly.

Opening Sealed Documents

OPEN THE SEALED ATTACHMENTS

After registering, you will also receive a second email with three attachments. Open each of these attachments and experience the different behavior depending on their level of security

- Announcement One.doc file – this is sealed to “L3 Company Announcements”. You have Reader rights and so you may only view company announcements on-screen. Try to edit, copy or print the information. Try to use Print Screen to capture an image. Look at the menu options available to you, you will see that many of the standard features are not enabled.
- Business Plan.doc file – this is sealed to “L2 Sales”. You are a Contributor to sales documents – you have full edit rights.
- Chairman’s Committee 07-March.ppt file – this is sealed to “L1 Board Communications”. You do not have any access rights to board documents at all! You have been displayed an online status page which has been configured to explain what document you have tried to open, why you have been denied access to it, what to do and who to contact if you believe you should have access to the document.

OPENING SEALED DOCUMENTS

If you have the Oracle IRM Desktop installed, you can simply double-click to open a sealed document.

The first time you open a sealed document, you might be challenged for the username and password of your IRM account, and you might be required to change your password. If you are challenged for a password, you can tick the Login automatically checkbox to ensure that you are not challenged next time.

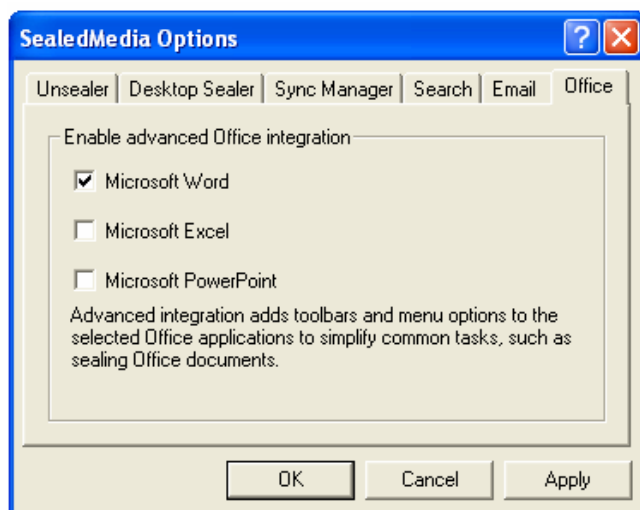
Having authenticated, the Oracle IRM Desktop checks with the Oracle IRM Server to see whether you have the right to open the sealed document. Typically, the administrator will make sure you have rights for the first document you receive. Once opened, your ability to interact with the document is controlled 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. This web page is customer-configurable, so it can include self-help information, email links to people who can help, and other context sensitive information.

Enabling Office integration

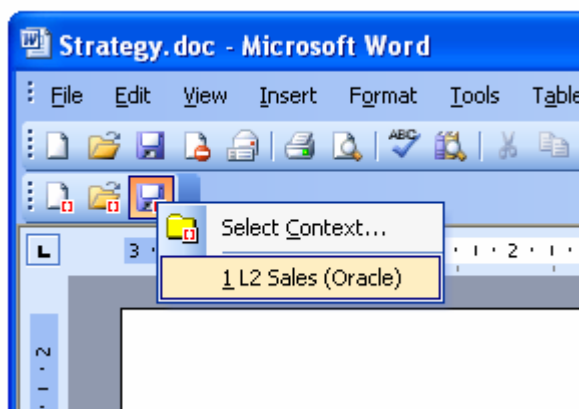
The Oracle IRM Desktop automatically supports the creation and editing of sealed Office documents, and controls Office to ensure that you do not accidentally exceed your rights. The Desktop can also provide more advanced Office integration. This might be enabled automatically. If not, you can enable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

1. Right-click on the SealedMedia icon  in your system tray on your Windows Desktop and select Settings.... The SealedMedia Options dialog will appear.
2. Select the **Office** tab of the SealedMedia Options dialog.



3. Tick the box for each Office application that you want to enable, and click **OK**.

The next time you start the selected applications they provide sealing-related options on the File menu and in a SealedMedia toolbar. For example, you can use the SealedMedia toolbar to seal a document as illustrated.



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

Sealing Documents

CLASSIFICATION OF DOCUMENTS

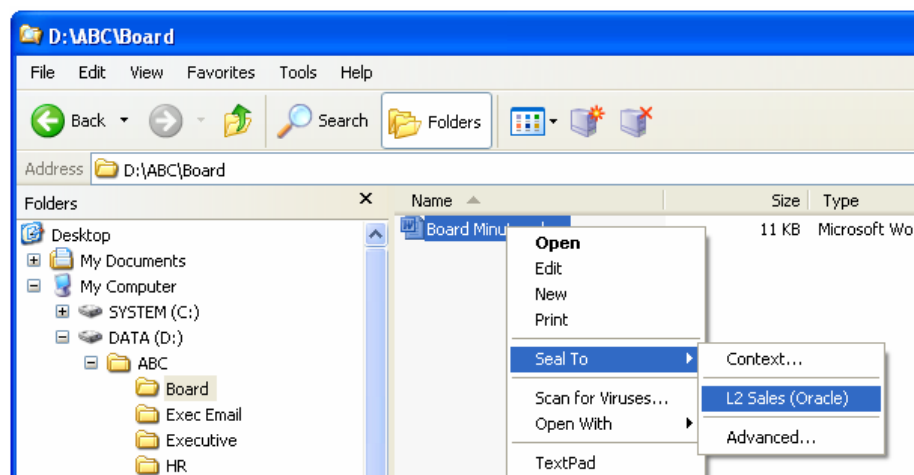
Oracle’s unique classification-based approach to rights management enables organizations to easily manage access to large volumes of sensitive information in terms of existing business processes or information classifications (such as “Board Communications L1” or “Company Confidential L3”), existing employee roles (such as “Reviewer” or “Contributor”), and existing users and groups defined in enterprise directories (such as “Sales”).

When sealing a document, or created a new sealed document, the classification of that document needs to be specified. The decision will depend on the sensitivity of the content of the document. The classification is determined by the Context that the document is sealed to.

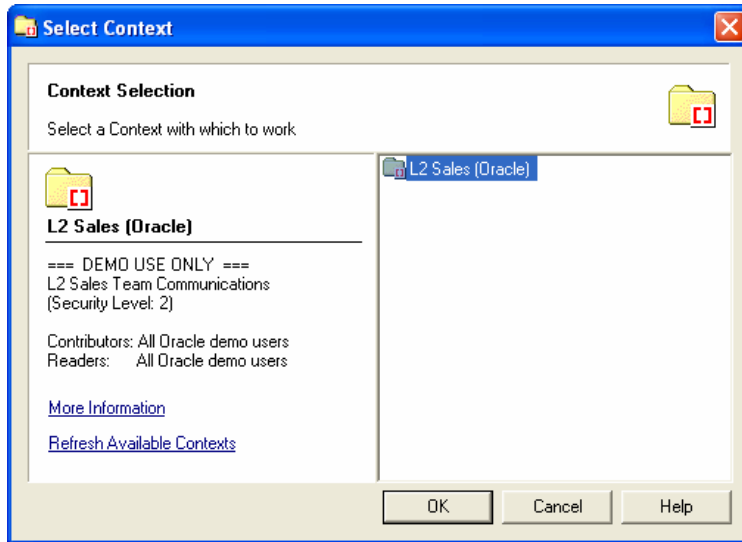
SEALING AN EXISTING DOCUMENT

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

1. Right-click on the document in Windows Explorer, and go to Seal To... Context.... This will enable you to select a security classification from those available to you.



A context selection dialog appears, as shown.



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 Available Contexts option to update it. A brief textual description can be configured for each Context, helping reinforce the user's understanding of the information classification policy.

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. By default the original document is not deleted, but the original can be removed as follows: After right-clicking on the file in Windows Explorer (as in 1 above) select Seal To > Advanced and choose your desired Context. Then click Ok and open the Options>> at the bottom right of the dialogue. Here you can opt to delete source files after sealing.

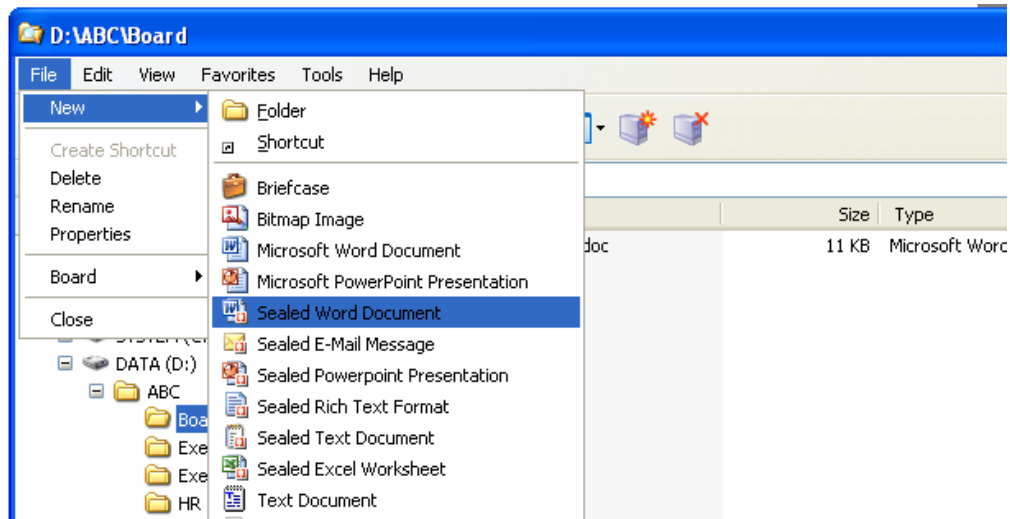
Alternatively, the Office integration provides sealing options within Office applications. In each case, the option requires to select a context as shown above.

CREATING A NEW BLANK SEALED DOCUMENT

New users of Oracle Information Rights Management often seal pre-existing documents. However more experienced users tend to seal documents at inception. This can be from using templates, cloning exiting documents, or because the content of the document is known to be sensitive from inception. You can create new blank sealed documents from the Windows Explorer File menu - just as you can create new unsealed documents.

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

1. In Windows Explorer, select the folder in which you want to create the new sealed document.
2. Select File – New – 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.

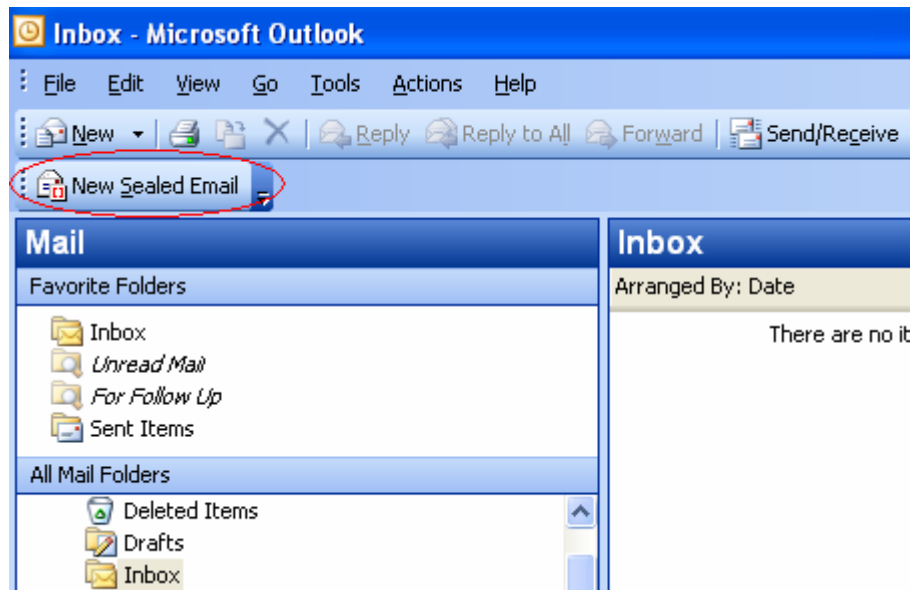
Alternatively, the Office integration provides toolbars and File menu options for creating new sealed documents within the Office applications. One of the great benefits of Oracle Information Rights Management is the consistency of the user interface across documents, email clients, Windows and Explorer ensuring high levels of usability.

Using Sealed Email

The Oracle IRM Desktop provides email integration for Microsoft Outlook, Lotus Notes and Novell GroupWise.

Please note. Integration with Outlook, GroupWise, and Notes is disabled by default, so you need to enable it as described in enabling Office integration earlier. You may need to restart your email application before these options become available.

Your email application now has sealing options integrated into it, for example, there is a New Sealed Email toolbar.



CREATE A NEW SEALED EMAIL

You can create sealed email in a number of ways, for example:

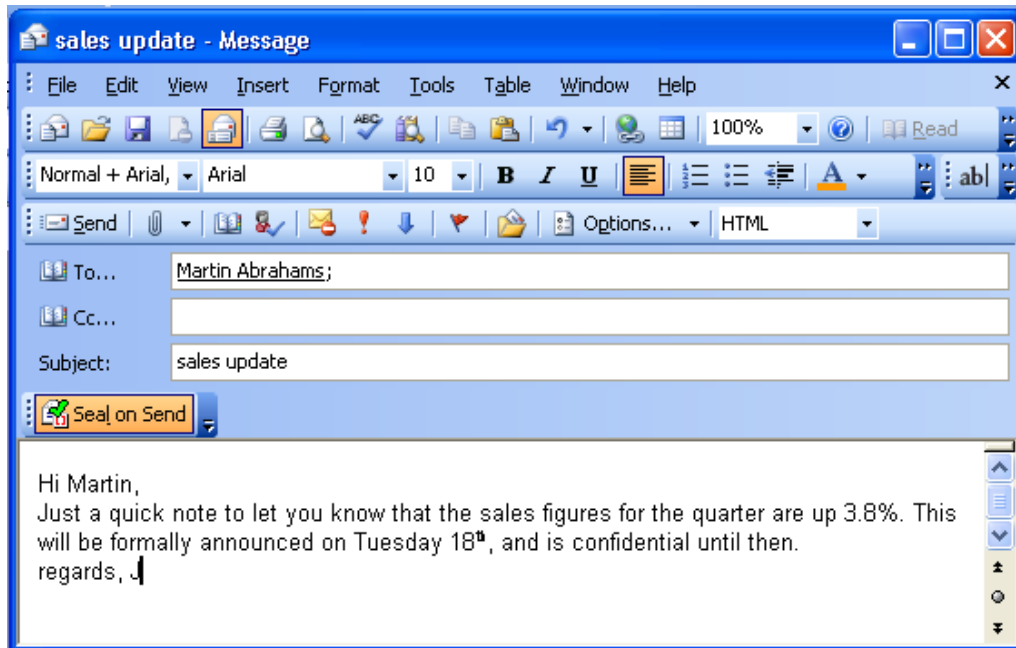
1. In your email application, click the New Sealed Email button.

For example, using Outlook:



2. Prepare your message as usual, and click Send. Note that the Seal on Send button is toggled active.

The Seal on Send toggle is permanently present, once enabled, within your standard email composition window. This enables you to decide that the content of an email, as you write it, has become sensitive and requires sealing. You are not forced to make this decision before you start, thus your normal workflow is not altered.



A context selection dialog appears, showing the list of contexts in which you have the right to seal. If you think the list is incomplete, you can use the Refresh Available Contexts option to update it.

3. Select a context and click OK.

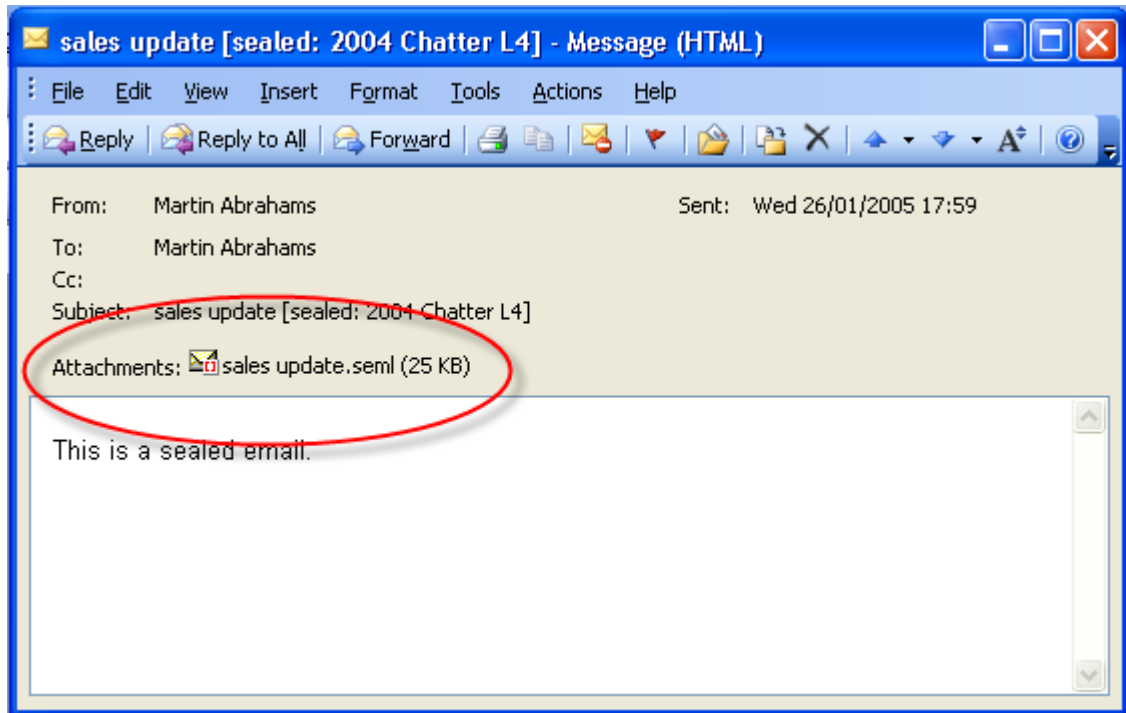
Your email is sealed to the selected context and sent to the user(s) specified in the address fields. Those users need to have the right to open documents in the selected context.


OPEN AND READ SEALED EMAIL

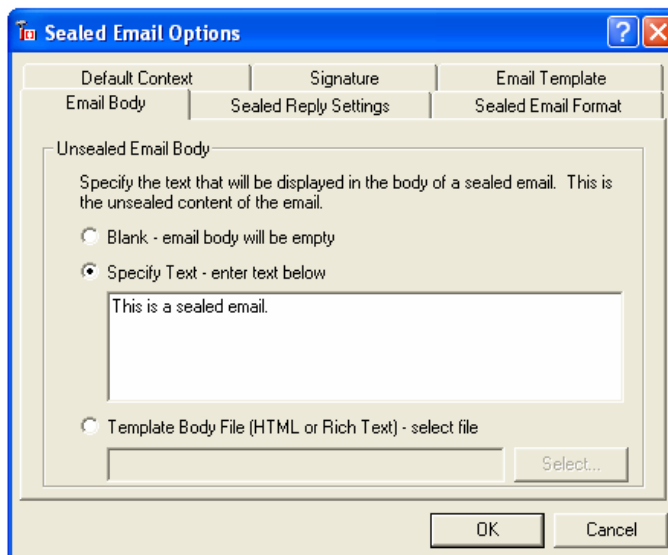
You can open and read sealed email, as follows:

1. Select the email in your Inbox as usual, and open it.

The email contains a sealed attachment.



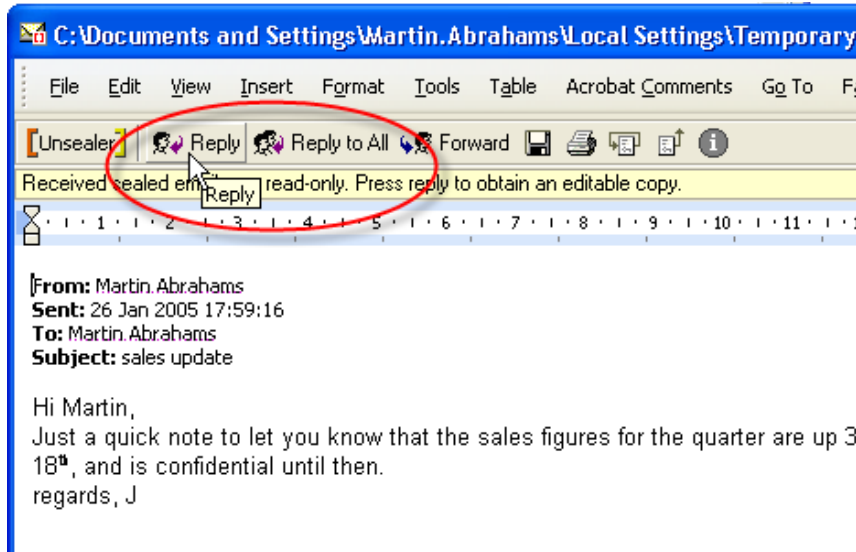
2. Select and open the sealed attachment. You need the right to open the email. The text in the email body, "This is a sealed email", is user-configurable from the options: right-click on the SealedMedia icon  in your system tray on your Windows Desktop and select Settings.... The SealedMedia Options dialog will appear. Select the Email tab, then click the Settings... button. Select Email Body in the pop-up and then edit the text, or attach an HTML file.



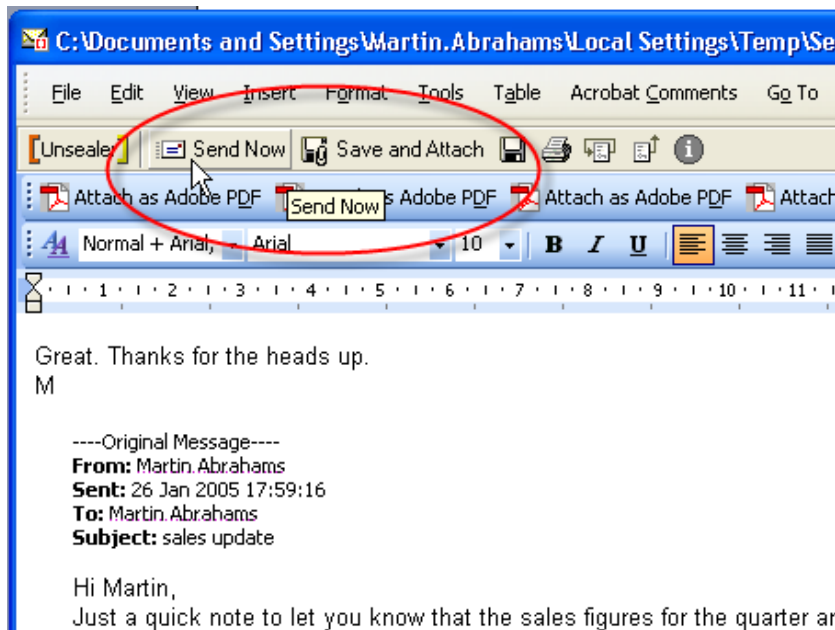
REPLY TO SEALED EMAIL

You can reply to a sealed email, as follows below. It should be noted that you need to open the sealed email attachment and reply from within this. If you reply directly from the parent email window, then the original content will not be appended and the reply will not be sealed by default.

1. Open the sealed email attachment and click Reply or Reply to All.



2. Edit the sealed attachment as required, subject to your rights.
3. When ready, click Send Now or Save and Attach.



If you click Send Now, the message is sent immediately.

If you click **Save and Attach**, the attachment closes and you are returned to the main email window so that you can amend the addressees, for example, before clicking **Send**.

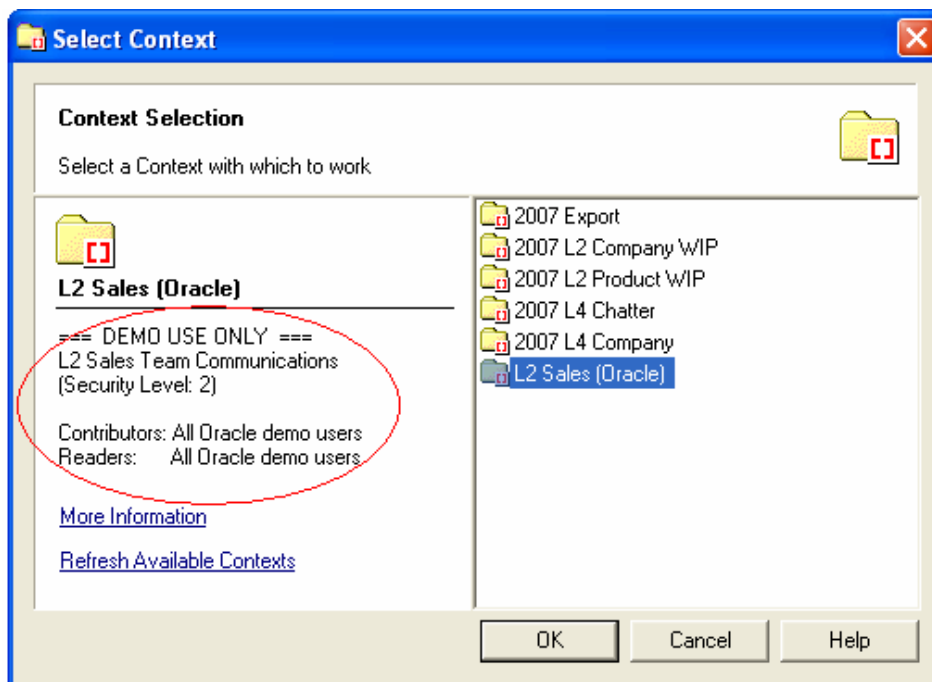
Only users who have the correct rights to access the classification that you have assigned to the email will be able to open it. Thus the distribution list of an email does not determine who can read it. This is a key benefit of the classification rights model, guarding against mis-addressing an email.

Accounts on Multiple Servers

Although you are evaluating Oracle Information Rights Management, you may already have used it in a business context. Perhaps a colleague, partner or publisher has already sent you sealed content which you have previously accessed. If this is the case then you may already have downloaded the Oracle IRM Desktop to your PC and connected to a different license server.

This will not affect this evaluation, but some of the screenshots used in this document may be slightly inaccurate for you. Most notably, if you have contributor rights on another server then you will see additional Contexts available for you to select when sealing content.

In the screenshot below, you will see that the “L2 Sales (Oracle)” context is now just one of several available for selection. Clicking each one of them will display the descriptive information in the left hand pane.



Summary

WHAT YOU HAVE EVALUATED

In this evaluation you should have been able to experience:

- Setting up an evaluation account.
- Downloading the Oracle IRM Desktop software and test your account.
- Receiving an email with sealed attachments. These were sealed to different classifications so you have experienced different rights.
- Enabling Oracle IRM Desktop integrations with Office, Outlook and Notes email.
- Sealing your existing documents and creating new sealed documents.
- Sending sealed emails, receiving sealed emails and replying to sealed emails.

If you have not already done so, why not ask your colleagues to request evaluation accounts, you can then share your own sealed documents and emails, gaining an enhanced appreciation of the evaluation.

NEXT STEPS

You have now experienced Oracle Information Rights Management from an end-user's perspective. You will now understand the ease of use, seamless integration into existing workflows, and can hopefully see the benefits to your business.

If you would now like a fuller evaluation, including experience of administration roles then please contact irm_evaluation_request_ww@oracle.com