Oracle® Fusion Middleware

External User Support Guide for Oracle IRM Desktop

11*g* Release 1 (11.1.1)

E12450-03

January 2011

ORACLE®

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

E12450-03

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 v

1 External User Support

1.1 What is Oracle IRM? 1-1
1.2 Approving Oracle IRM Client Software 1-2
1.2.1 Software Compatibility 1-2
1.2.2 System Security 1-2
1.2.3 Network Security Compatibility 1-2
1.2.4 Network Use Considerations 1-3
1.2.5 Virus Scanner Compatibility 1-3
1.2.6 Organizational Awareness of Document Content 1-3
1.3 Supported Platforms 1-4
1.4 Installation Considerations 1-4
1.5 Opening Sealed Documents 1-4
1.6 General Use Considerations 1-5
1.6.1 Executable Processes 1-5
1.6.2 Local Rights Caches 1-5
1.6.3 Extensions to Applications 1-5
1.7 Troubleshooting 1-6
1.7.1 External user is not allowed to use the internet 1-6
1.7.2 External user does not have the address of the download site 1-6
1.7.3 External user is using the wrong address for the download site 1-6
1.7.4 Originator's download site is temporarily unavailable 1-6
1.7.5 Downloads of executable files are blocked 1-6
1.7.6 External user does not have privileges to run installations 1-6
1.7.7 External user cannot authenticate 1-7
1.7.8 Oracle IRM Desktop cannot connect to Oracle IRM Server 1-7
1.7.9 Proxy settings are incorrect 1-7
1.7.10 Proxy server requires authentication 1-7
1.7.11 External user has no rights to the sealed document 1-7

Index

Preface

This guide is designed to make it easy to support anyone in your organization who receives a document or email that has been sealed using Oracle IRM, and who therefore needs to install the Oracle IRM Desktop client software.

Audience

This guide is primarily aimed at those who provide support for the recipients of sealed documents, or who authorize the use of software applications by such recipients.

This guide is specifically aimed at organizations that are not direct clients of Oracle.

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 documents:

- *Oracle Fusion Middleware User's Guide for Oracle IRM Desktop*
- *Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server*
- *Oracle Fusion Middleware Developer's Guide for Oracle IRM Server*

Conventions

The following text conventions are used in this document:

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

1

External User Support

This section includes the following topics:

- What is Oracle IRM?
- Approving Oracle IRM Client Software
- Supported Platforms
- Installation Considerations
- Opening Sealed Documents
- General Use Considerations
- Troubleshooting

1.1 What is Oracle IRM?

Oracle Information Rights Management (Oracle IRM, formerly SealedMedia E-DRM) is a type of information security solution that 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.

Oracle IRM 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 client software, 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 while they are in use within those applications.

Oracle IRM continues to protect and track sealed documents and emails when they are 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, and copying 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 Approving Oracle IRM Client Software

Oracle recognizes that many organizations have approval processes to ensure that software applications do not compromise network security, system stability, or general business rules. This section aims to provide information and assurances about the concerns that are typical during such an approval process.

1.2.1 Software Compatibility

Oracle IRM Desktop is exhaustively tested on a wide range of operating systems, and is tested for interoperability with a range of software applications, including the widely deployed versions of Microsoft Office, Microsoft Outlook, Microsoft Internet Explorer, Adobe Reader, and Lotus Notes.

Details of operating system and application support are available from the Oracle Information Rights Management Certification Information link on the Oracle IRM Downloads page of Oracle Technology Network.

1.2.2 System Security

The following key points should reassure you that system security will not be compromised by installing Oracle IRM Desktop:

- Oracle IRM Desktop maintains an encrypted and tamper-proof configuration cache.
- The communication protocol is encrypted and authenticated, and responses are not executable, so viruses cannot enter the company network via Oracle IRM Desktop.
- Oracle IRM Desktop never receives incoming connections, only responses to outbound connections.
- Sealed documents are not executable; they are encrypted versions of standard formats such as Microsoft Office, PDF, and HTML.
- Scripting in sealed HTML is subject to the same client-side controls as scripting in unsealed HTML.
- Any attempt to tamper with a sealed document is detected through the layer of encryption and digital signatures, causing Oracle IRM Desktop to refuse to open it.

1.2.3 Network Security Compatibility

Oracle IRM Desktop makes network connections to the Oracle IRM Server owned by the service host organization (the originators of the sealed documents or emails that people within your organization have received).

In security terms, communications with Oracle IRM Server are equivalent to browser communications with web servers. Oracle IRM Desktop communicates with 10g versions of Oracle IRM Server using a secure, encrypted variant of the HTTP protocol used by web browsers. For 11g versions of Oracle IRM Server, standardized HTTPS communications are used. Further:

- Oracle IRM Desktop never receives inbound connections — only responses from Oracle IRM Server and its associated web server.
- Oracle IRM Desktop does not keep TCP connections to Oracle IRM Server open.

- Oracle IRM Desktop never communicates with anything other than the Oracle IRM Server and its associated web server. Oracle IRM Desktop never communicates with, for example, other clients.
- All communications with Oracle IRM Server are encrypted and authenticated.
- Oracle IRM Desktop does not attempt to modify network settings to enable communications. Oracle IRM Desktop uses the proxy settings in Internet Explorer, if present, but does not attempt to change them.
- Oracle IRM Desktop provides a connection testing facility that can help diagnose connectivity issues, if required, but does not attempt to resolve those issues.

1.2.4 Network Use Considerations

Oracle IRM Desktop must periodically communicate with Oracle IRM Server to obtain decryption keys and licenses to use sealed documents. This communication needs to be permitted by any intervening firewalls.

In most cases firewalls need no special configuration because Oracle IRM Desktop uses the same network ports and protocols as web browsers. If users are already allowed access to the Internet, Oracle IRM Desktop can usually operate successfully without any additional network configuration.

By default, Oracle IRM Desktop automatically detects and uses Internet Explorer's proxy settings, which can be configured to use a designated proxy server, and to automatically authenticate to proxies, if required. If proxy authentication is not automatic, the user will be prompted to authenticate to the proxy manually.

If Oracle IRM Desktop experiences connectivity problems, it has a built-in network diagnostic test whose results can be used to make appropriate modifications to the network. Users can initiate this test by opening a sealed document, clicking on the Online Information icon on the toolbar, and clicking the Test link on the status page. Status pages open automatically if sealed content cannot be displayed because of a problem. A self-test reveals the address and port that Oracle IRM Desktop needs to be able to connect to. The firewall needs to allow connections and responses.

1.2.5 Virus Scanner Compatibility

Sealed documents are encrypted, which can (in extremely rare cases) cause a sealed document to contain what appears to be a virus signature. However, sealed documents are never executed, so they cannot transmit a virus.

Virus scanners might prevent users from downloading sealed documents because they have an unusual MIME type. To avoid this situation you might be able configure your virus scanner to recognize and accept the MIME types of sealed documents. The organization that originated the sealed document or email will be able to obtain a list of applicable MIME types from Oracle's Metalink support service.

1.2.6 Organizational Awareness of Document Content

Your organization may have a requirement to be aware of the content of all documents retained by it, even sealed ones (for example for legal or eDiscovery purposes). This requirement may be satisfied by using the Oracle IRM Desktop search component. Your organization will then be able to identify documents containing specific content and take any necessary action.

The Oracle IRM Desktop search component enables Windows search facilities and the Microsoft Indexing Service to search and index sealed documents, subject to the user's

rights. A particular user's search right will normally be confined to documents that the user has the right to read. Therefore, to implement this solution, it will be necessary to create a privileged user who has the search right to all sealed documents retained by your organization. (The privileged user need not have the right to read all such documents, only to search them.) You will need to contact the originator of the sealed documents to have them create the privileged user, with the necessary rights, and send the authentication details (username and password) to an appropriate person within your organization.

1.3 Supported Platforms

Oracle IRM Desktop supports a very wide range of operating systems and browsing/rendering software. For the latest information about supported platforms, please refer to the Technology Characteristics and Specifications datasheet freely available from the Oracle Technology Network web site.

Oracle IRM Desktop must not be installed on an Exchange Server. The application uses the .stm file extension, so installing Oracle IRM Desktop can impact mail services. There should be no reason to install on an Exchange Server, as the Oracle IRM applications are client software intended for end user systems.

1.4 Installation Considerations

Oracle IRM Desktop installation is very simple, and does not ask users any questions that require specialist knowledge.

Oracle IRM Desktop is freely available from the Oracle IRM downloads area on the Oracle Technology Network web site. The *Oracle IRM Desktop User's Guide* (which covers installation of the software) is also available from the same location.

External users may receive an invitation to download the Oracle IRM Desktop software from a web page provided by the originator of a sealed document or email. This typically invokes the Oracle IRM download wizard hosted on the Oracle IRM download site, although the redirection to this site may not be apparent to the user.

To install the package, users need administrative privileges. They also require privileges to modify the registry.

If you are installing Oracle IRM Desktop on a server in a Citrix environment, you must use the Add & Remove Programs dialog of the Windows Control Panel, rather than run the installer simply by double-clicking it. If you are installing on a Citrix server farm, you need to install on each server. The Oracle IRM Desktop User's Guide (available from the Oracle IRM documentation download web site) describes the installation and use of Oracle IRM software in a Citrix environment.

1.5 Opening Sealed Documents

After installing Oracle IRM Desktop, the final step is to open a sealed document. Users do not specifically run Oracle IRM Desktop — the client software runs automatically when the user tries to open sealed documents.

Users can receive sealed documents in many ways, including as email attachments or as files downloaded from a web server. The first time that a user attempts to open a sealed document, Oracle IRM Desktop attempts to communicate with the host organization's Oracle IRM Server to get the user's rights to open the document. Most of the time this succeeds without incident. However, see the Troubleshooting sections for potential issues that can arise.

1.6 General Use Considerations

This section describes the executable processes and local rights caches to which users must have access, and describes the extensions to applications provided by Oracle IRM Desktop.

1.6.1 Executable Processes

Oracle IRM Desktop uses a process called `IrmBackground.exe` for a variety of activities. This process automatically starts when the user logs in. The user account must be able to run this executable.

`OracleIRMServiceHost` is installed as a service to enable indexed search.

1.6.2 Local Rights Caches

Oracle IRM Desktop manages local rights caches, one per user, on the user's system.

For Windows XP and Windows Server 2003, the local rights cache is in the following folder:

```
%USERPROFILE%\Local Settings\Application Data\Oracle
```

For Windows Vista, Windows 7, and Windows Server 2008, the local rights cache is in the following folder:

```
%LOCALAPPDATA%\..\LocalLow\Oracle
```

Additionally, for indexed search, Oracle IRM Desktop manages a system-wide cache in the following folder:

```
%ALLUSERSPROFILE%\Oracle\IRM
```

The user account needs full access to the appropriate folder.

1.6.3 Extensions to Applications

Oracle IRM Desktop provides extensions to applications as follows:

- **Microsoft Office support.** The Microsoft Office component integrates sealing options into Microsoft Word, Microsoft Excel, and Microsoft PowerPoint.
- **Sealing in Windows Explorer**. The Oracle IRM Desktop sealing component is a standard Windows shell extension. The shell extension adds sealing-related options to Windows Explorer. For example, if the Oracle IRM Desktop sealing component is enabled, the Windows Explorer File menu offers options to seal and reseal documents of supported formats.
- **Searching in sealed documents**. The search component installs a standard file filter that enables Windows search facilities and the Microsoft Indexing Service to search and index sealed documents, subject to the user's rights.
- **Email integration.** The Email component integrates sealing options into Microsoft Outlook and Lotus Notes. This enables users to send sealed emails and reply to them, subject to the user's rights.
- **Internet Explorer.** Oracle IRM Desktop adds a browser plugin to enable Internet Explorer to display sealed HTML and PDF documents.

By default, the Microsoft Office component, the Oracle IRM Desktop sealing component, and the search component are enabled, whereas email integration is not. These components can be enabled or disabled from the Oracle IRM Desktop Options dialog.

1.7 Troubleshooting

This section describes common issues and their solutions.

1.7.1 External user is not allowed to use the internet

If your organization does not permit Internet access at all, arrangements can be made with the originator of the sealed document or email to distribute the client software by other means. However, Oracle IRM Desktop needs to be able to connect to Oracle IRM Server and a web server, so arrangements need to be made to enable connection to the relevant service addresses. If only one or two individuals require the use of Oracle IRM Desktop, it might be more practical to make private arrangements for them to use the software from a home computer.

1.7.2 External user does not have the address of the download site

Typically, intended recipients of a sealed document receive an introductory email, or similar communication, that includes the URL of the site from which the Oracle IRM Desktop software can be downloaded. If this is not the case, and someone receives a sealed document with no covering information, attempting to open the sealed document will usually result in a link to the Oracle IRM Desktop download web site. This is because the file extensions of sealed documents (sdoc, sxls, sppt, for example) are registered and, in most cases, when a user attempts to open a sealed document, the operating system helps them find a suitable application.

1.7.3 External user is using the wrong address for the download site

Intended recipients normally receive the address from which the Oracle IRM Desktop software can be downloaded in an introductory email, ideally as a link that they can click on. If the address does not work, check the address has been received correctly, and that no error has been made copying the address into a browser address toolbar.

1.7.4 Originator's download site is temporarily unavailable

If the originator's site for downloading the Oracle IRM Desktop software is unavailable, contact them so that they can correct the fault.

1.7.5 Downloads of executable files are blocked

The download is an executable file. Your organization may run firewalls and proxy servers that do not permit users to download executable files, or restrict the set of web sites from which downloads are permitted. In this case, the download site can be added to the list of permitted sites. If this is not permissible, contact the originator of the sealed document or email to make other arrangements to obtain the Oracle IRM Desktop software.

1.7.6 External user does not have privileges to run installations

The Oracle IRM Desktop software download site encourages the intended recipient to open or run the download, and doing so automatically starts the installation. If, however, this user does not have sufficient privileges to run the installation, assistance from a local administrator will be required.

1.7.7 External user cannot authenticate

In most cases, the intended user of a document needs a username and password to authenticate to Oracle IRM Server. Typically, this username and password is received in an introductory email or similar communication.

If the username and password are rejected, check that they have been typed correctly. Passwords are case-sensitive; usernames are not.

If the user has forgotten both their username and password, contact the originator of the sealed document or email so that new ones can be issued.

1.7.8 Oracle IRM Desktop cannot connect to Oracle IRM Server

In the event of connection failure, the Oracle IRM Desktop status page opens. The page contains a test link that enables a user to test connectivity to the Oracle IRM Server. In case of problems, contact the organization from which the sealed document or email originated.

1.7.9 Proxy settings are incorrect

Oracle IRM Desktop uses the Internet Explorer proxy settings. In most cases, if Internet Explorer can access the Internet successfully, then Oracle IRM Desktop can connect to Oracle IRM Server.

1.7.10 Proxy server requires authentication

Your organization might have a proxy server that requires users to authenticate when connecting to external networks. In many cases, this authentication is automated as part of the proxy settings. However, if manual authentication is required, users need to know what credentials to use. The client cannot connect unless the user authenticates to the proxy server.

1.7.11 External user has no rights to the sealed document

Typically, users receive sealed documents that are intended for them, and the first document they receive is particularly likely to be intended for them. However, it is always possible for a user to receive a document that they do not have the right to open. This results in a user authenticating successfully, but being refused access to the document. The user should contact the originator of the sealed document or email to resolve the matter.

Index

A

applications
  extensions to, 1-5
approval processes, 1-2
authentication
  problems, 1-7
  proxy server, 1-7

B

blocked downloads, 1-6

C

caches
  for search indexes, 1-5
  local, 1-5
compatibility
  network security, 1-2
  software, 1-2
  virus scanners, 1-3
connection failure, 1-7

D

document content
  organizational awareness of, 1-3
download site
  address unknown, 1-6
  temporarily unavailable, 1-6
  wrong address for, 1-6
downloads
  blocked, 1-6

E

email integration, 1-5
exchange server, 1-4
executable files
  blocked from download, 1-6
executable processes, 1-5
extensions to applications, 1-5

I

indexed searches, 1-5
installation
  considerations, 1-4
  no privileges, 1-6
internet
  use not allowed, 1-6
Internet Explorer, 1-5

L

local rights caches, 1-5
Lotus Notes, 1-5

M

Microsoft Indexing Service, 1-5
Microsoft Office integration, 1-5
Microsoft Outlook, 1-5

N

network
  security, 1-2
  use, 1-3

O

opening sealed documents, 1-4
Oracle IRM, 1-1

P

platforms, 1-4
privileges required, 1-6
processes
  executable, 1-5
proxy server, 1-7
proxy settings, 1-7

R

rights, 1-7

S

sealed documents
  no user rights, 1-7
  opening, 1-4

search indexing, 1-5
security
  network, 1-2
  system, 1-2
software compatibility, 1-2
specifications datasheet, 1-4
supported platforms, 1-4
system security, 1-2

T

troubleshooting, 1-6

V

virus scanners, 1-3

W

Windows Explorer, 1-5